Дапаможнік Вожыка-актывіста

Усталяваньне і выкарыстаньне праграмаў, карысных для бясьпекі

Менск, 2012





Гэтае выданьне зьяўляецца працягам і разьвіцьцём “Кансьпіратара Беларускага” – дапаможніка для грамадзкіх актывістаў, упершыню выдадзенага ў 2005 г.

Мы дзякуем за дапамогу ў ажыцьцяўленьні праекту калегам са славацкай грамадзкай арганізацыі Človek v ohrození.

Наклад 299 асобнікаў.

Зьмест

частка

A

Абарона носьбітаў інфармацыі і сродкаў камунікацыяў

Абарона носьбітаў інфармацыі і сродкаў камунікацыяў

Перад тым як даваць парады, зьвязаныя з вылічальнай тэхнікай і праграмнымі тэхналёгіямі, вызначым нашыя базавыя паняткі «*давер*» і «*надзейнасьць*» у кантэксьце гэтае тэмы.

Праграма вартая даверу, калі яна дастаткова ***распаўсюджаная*** (маецца на ўвазе ў кампутаровым сьвеце, бо распаўсюджанасьць, напрыклад, у Буда-Кашалёве ці нават у Менску нельга ўспрымаць як сур'ёзны аргумэнт), калі яе ***код даступны*** для праверкі кожнаму, хто пажадае (у прафэсійнай тэрміналёгіі open-source, праграмы з адкрытым кодам), калі дыстрыбутыў (інсталяцыйны дыск) атрыманы ***з вартых даверу крыніцаў.***

Ня варта захапляцца скачваньнем розных цікавых праграмак з Інтэрнэту, бо існуе шмат сайтаў, дзе вы разам з крэкнутымі праграмамі атрымаеце ў дадатак пару-тройку траянаў.

Калі йдзецца пра сродкі шыфраваньня і забесьпячэньня электроннае бясьпекі, пірацкі дыск, куплены з латка ці нават у краме, не зьяўляецца вартай даверу крыніцай!

Такія праграмы трэба выладоўваць з Інтэрнэту з сайту вытворцы ці купляць праз замежныя Інтэрнэт-крамы. Інакш вы рызыкуеце нарвацца на запушчаную спэцслужбамі ці проста нягоднікамі фальшыўку, якая будзе ўтрымліваць шпегаўскія «закладкі».

Абсалютна надзейных праграмаў практычна не існуе, але больш-менш надзейнымі можна лічыць тыя, што былі праверяныя прафэсіяналамі ў галіне кампутаровай бясьпекі.

І яшчэ адна папярэдняя заўвага: усе тэхнічныя сродкі бясьпекі інфармацыі і камунікацыі мала чаго вартыя, калі ў арганізацыі пануе бязладзьдзе, адсутнічае дысцыпліна і не выконваюцца дырэктывы начальства.

Калі на штаб-кватэры тусуюцца невядомыя асобы, арганізоўваюцца

п’янкі і гулянкі з запрашэньнем ненадзейных, сумнеўных і патэнцыйна варожых элемэнтаў - выдаткаваныя на бясьпеку сродкі будуць простым марнатраўствам.

Як захоўваць інфармацыю на кампутары?

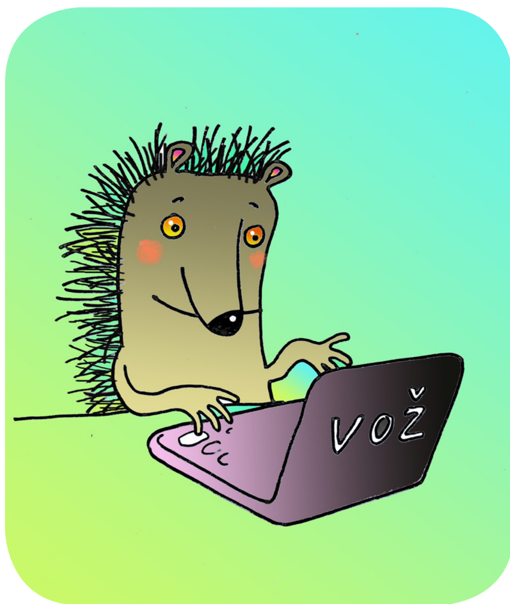
Працу сучаснай арганізацыі немагчыма ўявіць без шырокага выкарыстаньня кампутарнай тэхнікі. У большасьці беларускіх арганізацыяў менавіта на кампутарах, а не на паперы, зьмяшчаюцца масівы інфармацыі, у тым ліку канфідэнцыйнай, якая можа зацікавіць спэцслужбы. Часам гэтая інфармацыя можа стаць падставай для прыцягненьня да адміністрацыйнай альбо нават крымінальнай адказнасьці - у дзейнасьці беларускіх няўрадавых арганізацыяў ужо былі гэткія выпадкі.

Захоўваньне інфармацыі на кампутары больш зручнае для працы, чым захоўваньне яе ў папяровым выглядзе, а таксама ў нейкім сэнсе больш бясьпечнае. Гэта зьвязана з тым, што інфармацыю ў электронным выглядзе значна прасьцей зашыфроўваць і перазашыфроўваць, чым інфармацыю на папяровых носьбітах.

Такім чынам, галоўнае правіла, якім трэба карыстацца пры працы на кампутары, - шыфруй! Ваш прыватны кампутар можа быць скрадзены альбо выняты ці канфіскаваны спэцслужбамі, а таксама існуе небясьпека, што да яго могуць атрымаць доступ непажаданыя пэрсанажы. Таму абавязкова трэба карыстацца сродкамі шыфраваньня інфармацыі.

Шыфраваць можна як асобныя файлы, гэтак і цэлыя дыскі. Існуюць таксама «віртуальныя шыфраваныя дыскі» (далей ВШД) - гэта вялікія файлы, якія ўнутры сябе зьмяшчаюць у зашыфраваным выглядзе мноства іншых файлаў. Гэта падобна да zip- ці rar-архіву, адрозьненьне ў тым, што адмысловыя праграмы дазваляюць адчыніць (у кампутаровай тэрміналёгіі «змантаваць») іх так, што зь зьмесьцівам гэтых файлаў можна працаваць як з асобнымі дыскамі (ці каталёгамі), пры гэтым сыстэма аўтаматычна шыфруе тое, што вы пішаце на свой віртуальны дыск, і расшыфроўвае тое, што вам трэба прачытаць.

Па заканчэньні працы вы зачыняеце (дэмантуеце) дыск - і інфармацыя становіцца недаступнай. Апісаны парадак працы карысны для няўрадавых арганізацыяў: кожны супрацоўнік мае свой за-



шыфраваны дыск і толькі ён ведае пароль ад гэтага дыску. Такім чынам дасягаецца дастаткова вялікая ступень карпаратыўнай бясьпекі - ня толькі праз тое, што праца кожнага з карыстальнікаў зашыфраваная і не даступная для «ворагаў», але таксама і праз тое, што супрацоўнікі ведаюць толькі свой сэгмэнт інфармацыі і ня маюць паролю для іншых ВШД. Бадай што, ВШД - адзін з аптымальных сродкаў працы зь вялікай колькасьцю важных файлаў.

Варта згадаць пра такі мэтад абароны інфармацыі, як стэганаграфія. Спрошчана, гэта спосаб схаваць канфідэнцыйную інфармацыю, незаўважна ўнятрыўшы яе ў несакрэтную. Напрыклад, стэганаграфічным зьяўляецца тэкст тэлефанаваньня «Трэба ехаць у Гальшаны - бабуля ўжо нагатавала сочыва зь яблыкаў» - хто ведае, што ў гэтых бяскрыўдных словах схаванае паведамленьне «Ў падпольнай друкарні выраблены наклад улётак».

Аналягічна і ў кампутаровай інфармацыі сакрэтнае паведамленьне можна прыхаваць у несакрэтным файле. З гэтай магчымасьці мае сэнс скарыстацца ў выпадку, калі трэба ня проста абмежаваць доступ да інфармацыі, але зрабіць сам факт яе існаваньня таямніцай. Напрыклад, файл з дакумэнтам можна «ўплесьці» ў карцінку (здымак з рыбалкі), фільм ці музычны трэк, прычым выніковая карцінка візуальна ня будзе адрозьнівацца ад арыгінальнай, фільм можна будзе глядзець, а музыку слухаць, анічога асаблівага не заўважыўшы. Зразумела, гэты мэтад мае свае заганы.

Асноўная - каб сакрэтны файл сапраўды незаўважна «расчыніўся» ў нетрах падстаўнога, памер апошняга мусіць быць сама меней у 15-20 разоў большы за памер сакрэтнага. Так што калі вы будзеце хаваць вялікія файлы, дыскавая прастора будзе выдаткоўвацца вельмі неэка-

номна, апроч таго, можа ўзьнікнуць праблема знайсьці падстаўны файл патрэбнага памеру.

Калі вы выкарыстоўваеце пакарыстацца стэганаграфічнымі праграмамі, паклапаціцеся пра тое, каб аніхто ня выдаліў тых файлаў, у якіх таемна захоўваецца вашая інфармацыя (нехта ж можа без асаблівага клопату паставіцца, напрыклад, да музычнага файлу і выдаліць яго, каб вызваліць месца на дыску).

Паролі

Паролі для шыфраваньня - калі вы не падыдзеце да гэтага пытаньня адказна - стануць вашай праблемай.

Прыдумаць пароль для шыфравальнай праграмы - гэта сур'ёзная задача! Сучасныя сыстэмы ўзлому здольныя з высокай хуткасьцю перабіраць розныя варыянты пароляў з выкарыстаньнем слоўнікаў.

Дапрыкладу, уявім грамадзкага актывіста, які дзеля прастаты ўзяў за пароль нейкае слова.

Нават калі слова рэдкае - гэта пракол, бо прабегчыся па слоўніку праграма-ўзломнік зможа досыць спрытна. Хутчэй за ўсё, дастаткова будзе перабраць колькідзясят тысячаў варыянтаў, а гэта зусім няшмат для сучаснай кампутарнай тэхнікі.



Дадайце да гэтага, што ў праграму могуць быць уведзеныя вашыя пэрсанальныя зьвесткі (прафэсія, любімая музыка, імёны сямейнікаў і сяброў, хобі і г. д.), і гэта дазволіць расставіць прыярытэты і звузіць дыяпазон пошуку. Такім чынам, калі вы выкарыстоўваеце мянушку вашага сабакі ці дзень нараджэньня жонкі ў якасьці паролю - ведайце, для яго ўзлому можа хапіць некалькіх сэкундаў.

Надзейны пароль - доўгі (даўжыня залежыць ад канкрэтнага выпадку, але ў кожным разе ня менш за 8 знакаў), ніякай лёгікай ня зьвязаны з вамі і складзены з розных сымбаляў: літараў, лічбаў і спэцыяльных пазнакаў (накшталт ~ @ # &). Выкарыстоўвайце вялікія і малыя літары. Прыклад добрага паролю: Qni/u@917-GoX62. Ён нічога ня значыць, яго немагчыма вылічыць альбо падабраць з слоўніка, хіба толькі зрабіць перабор знакаў, але ж у такім разе колькасьць варыянтаў будзе занадта вялікай.

Відавочна, што надзейны пароль нялёгка запомніць, і ў выпадку, калі вам даводзіцца апэраваць мноствам складаных пароляў - хутчэй за ўсё так і будзе, - сытуацыя можа выйсьці з-пад кантролю. Многія людзі пачынаюць занатоўваць свае паролі на паперы - і гэта вельмі-вельмі кепска, бо паперкі маюць уласьцівасьць губляцца, вы можаце забыцца альбо пакінуць без нагляду свой нататнік, а ў выпадку непасрэдных рэпрэсіяў вас абшукаюць і ўсе падазроныя запісы будуць вывучаныя.

Хочацца папярэдзіць, што бальшыня нібыта хітрых прыёмаў - напрыклад укласьці паперку з паролямі пад акумулятар мабільніка альбо занатаваць эсэмэскай у памяці тэлефона - насамрэч былі правальнымі яшчэ да таго, як вы іх «вынайшлі».

З гэтага тупіка існуе выйсьце:

Захоўваць паролі ў спэцыяльнай праграме (можна парэкамэндаваць KeePass), у гэтым выпадку вы цьвёрда завучваеце адзін пароль, што адкрывае доступ да праграмы, якая ў сваю чаргу падказвае вам усе астатнія.

Апошняя парада - час ад часу мяняць паролі. У гэтым выпадку, у прынцыпе, можна карыстацца праграмамі - стваральнікамі пароляў.

Рэкамэндаваныя праграмныя сродкі для шыфраваньня

Ня трэба спадзявацца на магчымасьць проста «запароліць» файлы (альбо ўключэньне кампутара) стандартнымі сродкамі - варта выкарыстоўваць спэцыяльныя крыптаграфічныя (шыфравальныя) праграмы.

Няхай вас не бянтэжыць магчымае хуткае ўвядзеньне ў Беларусі адміністрацыйнай адказнасьці за парушэньне правілаў абароны інфармацыі - яна, хутчэй за ўсё, ня будзе датычыцца абароны асабістай прыватнай інфармацыі і рэальна ня будзе дзейнічаць.

Такім чынам, мы пачынаем ствараць на нашым кампутары зашыфраваны дыск.

Сродкі карыстаньня ВШД

У бальшыні сытуацыяў, найлепшым варыянтам - на час падрыхтоўкі нашага тэксту - зьяўляецца TrueCrypt - бясплатная праграма з добрай рэпутацыяй. Яна працуе на Windows, Linux, MacOS, з пэўнымі абмежаваньнямі на FreeBSD/PC-BSD.

Калі вы карыстаецеся Unix-падобнымі сыстэмамі, дык для стварэньня віртуальнага шыфраванага дыску (ВШД) вы маеце шмат сродкаў, іх апісаньне, аднак, выходзіць за межы гэтага матэрыялу.

Рэзэрвовая копія

Калі ваш кампутар (ваш дыск, іншы носьбіт інфармацыі) будзе скрадзены альбо канфіскаваны, ліхадзеі альбо «праваахоўнікі» будуць мець вашыя файлы, калі вы ігнаравалі патрабаваньні бясьпекі, і ня будуць нічога мець, калі інфармацыя надзейна зашыфраваная. Аднак глянем на сытуацыю зь іншага боку - вы таксама ня будзеце мець вашых файлаў! Нечакана (а такія рэчы заўсёды адбываюцца нечакана) апынуцца без дакумэнтаў, архіваў, базаў зьвестак, перапіскі, сьпісу кантактаў, уласных плянаў і напрацовак - гэта амаль заўсёды азначае параліюш арганізацыі і страты, часьцяком незваротныя.



Каб спаць спакойна, трэба ня толькі пазбавіць ня вартых даверу людзей доступу да інфармацыі, але й забясьпечыць надзейны доступ для сябе ў экстраардынарных сытуацыях. Для гэтага абавязкова трэба рабіць пэрыядычныя рэзэрвовыя копіі

ўсіх важных зьвестак (зразумела, таксама ў зашыфраваным варыянце) - напрыклад, раз на паўгоду рабіць рэзэрвовую копію ўсяго таго, што было напрацавана арганізацыяй.

Важна! Сакрэтная інфармацыя запісваецца на рэзэрвовы носьбіт-копію толькі ў зашыфраваным выглядзе! Калі вы карыстаецеся віртуальнымі шыфраванымі дыскамі - найпрасьцей капіяваць увесь файл, які ўтрымлівае дыск. Адсюль вынікае яшчэ адна парада - ствараючы ВШД, вызначайце яго памер ня большым за ёмістасьць носьбіта, на які вы звычайна робіце копію. Заўсёды правярайце, ці запісалася копія без памылак. Праграмы, што запісваюць CD і DVD, звычайна маюць опцыю «праверыць запіс» (анг. verify), - абавязкова ўключыце яе.

Захаваньне рэзэрвовых копіяў



Няма нічога дурнейшага, як зрабіць рэзэрвовую копію і пакінуць яе каля кампутара - у гэтым папросту няма ніякага сэнсу, менты альбо рабаўнікі ў выпадку форс-мажору атрымаюць і асноўную, і рэзэрвовую копію. Высnова: копіі трэба перахоўваць у іншым памяшканьні. Ці можна папросту забраць іх дахаты?

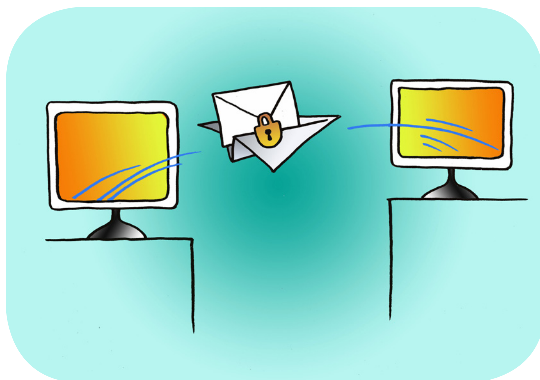
У прынцыпе, мы ня ведаем - пакуль - выпадкаў, калі б вобшукі ці крадзяжы праводзіліся адначасова ў офісах і прыватным жытле актывістаў. Аднак такое можа адбыцца заўтра - гэта ўваходзіць у лемантар «праваахоўнай» дзейнасьці спэцслужбаў. Ня варта захоўваць рэзэрвовую копію ў офісе іншай няўрадавай арганізацыі ў вашым горадзе - выпадкі правядзеньня некалькіх адначасовых вобшукаў у офісах некалькіх арганізацыяў ужо былі зафіксаваныя.

З тых жа прычынаў ня варта захоўваць рэзэрвовыя копіі ў офісах арганізацыяў, якія ўваходзяць у адну сетку. Найлепшы варыянт - аддаць іх надзейнаму чалавеку, які не працуе ў вашым офісе стала, альбо

захаваць іх у надзейнага сябра. Можаце рабіць некалькі копіяў адначасова і захоўваць іх у розных месцах - гэта павялічвае абсяг працы, але імавернасьць поўнага зьнікненьня інфармацыі ў такім разе блізкая да нулю.

Каб вырашыць, ці трэба вам гэта, уявіце сябе ў сытуацыі, калі вашая інфармацыя зьнікла, - наколькі гэта страшна менавіта для вас?

Як карыстацца электроннай поштай?



Інфармацыю зручна перасылаць праз электронную пошту, аднак вашыя лісты лёгка могуць быць перахопленыя. Для таго каб захоўваць бясьпеку, вам трэба карыстацца PGP альбо GPG - абедзьве праграмы ўзаемазамяняльныя.

Абменьвайцеся з вашымі карэспандэнтамі ключамі, шыфруйце файлы, якія перасылаеце, і пачувайце сябе бясьпечна - ніхто вашую перапіску напэўна не прачытае. Але пры гэтым захоўваецца небясьпека, што «ворагі» будуць ведаць, паміж якімі з «падазроных» паштовых скрыняў ідзе актыўная перапіска з выкарыстаньнем PGP альбо GPG, - часам гэта зьяўляецца непажаданым (напрыклад калі вы перапісваецеся зь нейкім вядомым замежным карэспандэнтам).

У мэтах прадухіленьня гэткай небясьпекі варта завесьці для асабліва канфідэнцыйнай перапіскі адмысловыя паштовыя скрыні. Калі вам трэба пераслаць асабліва канфідэнцыйную інфармацыю - вядома, зашыфраваную, - варта стварыць выключна дзеля гэтага выпадку спэцыяльную паштовую скрыню, якой вы скарыстаецеся толькі адзін раз з калектыўнага» выхаду ў Інтэрнэт (напрыклад, з інтэрнэт-кавярні).

Таксама пры карыстаньні электроннай поштай варта карыстацца самымі простымі правіламі асьцярожнасьці - націскаць «выхад» («sign out» альбо «log out») перад тым, як зачыніць старонку з поштай, выкарыстоўваць найбольш бясьпечныя зь існых на вашым сэрвэры

варыянтаў падлучэньня (напрыклад, для карыстальнікаў паштовага сэрвісу Yahoo! прапануецца два віды падлучэньня - стандартны і бясьпечны (secure) - мэтазгодна карыстацца апошнім), пэрыядычна мяняць паролі, не карыстацца простымі паролямі, не паведамляць пароль праз тэлефон і не казаць іншым людзям.

Натуральна, вельмі небясьпечна карыстацца паштовымі сэрвісамі, што даступныя для беларускіх спэцслужбаў, напрыклад tut.by, а таксама ня варта перасылаць на тутбаеўскія скрыні канфідэнцыйную інфармацыю.

Існуюць таксама паштовыя сэрвэры, якія маюць убудаваную сыстэму шыфраваньня, адзін з найбольш вядомых - hushmail.com. Не было б нічога дзіўнага, калі б высьветлілася, што за гэтымі сэрвэрамі стаяць спэцслужбы ЗША ці Брытаніі, аднак для нас гэта вялікай ролі ня грае: абы ня нашыя «добразычліўцы».

У працы з электроннай поштай існуе некалькі простых і надзвычай важных правілаў: ніколі не адчыняйце дадаткаў (attachments) няяснага альбо (нібыта) забаўляльнага прызначэньня, у тым ліку мульцікаў, праграмаў ды архіваў, пароль да якіх прапануецца ў целе ліста.

Даведнік тэрміналёгіі PGP/GPG

Ключ (key) - гэта зьвесткі, неабходныя для зашыфроўкі ці расшыфроўкі інфармацыі. Захоўваюцца ў файлах.

Памер ключа (key size) - памер таго пакету зьвестак, які зьяўляецца ключом. Чым большая даўжыня ключа, тым больш часу і высілкаў неабходна зламысьніку, каб яго падабраць. Вымяраецца ў бітах.



Адкрыты (ці публічны) ключ (public key) - ключ, якім можна толькі зашыфроўваць інфармацыю. Вы павінны распаўсюдзіць гэты ключ сярод тых, хто будзе пісаць вам шыфраваныя лісты.

Сакрэтны (ці прыватны) ключ (private key) - ім можна расшыфроўваць інфармацыю, зашыфраваную адкрытым ключом. Сакрэтны ключ - толькі для вас, ахоўваце яго ад пабочных асобаў. На выпадак, калі яго ўсё-ткі скрадуць, сыстэма PGP прадугледжвае пароль, ня ведаючы якога, сакрэтным ключом не скарыстаешся.

Адбітак ключа (key fingerprint) - даволі доўгі набор ангельскіх словаў, унікальны для кожнага ключа. Рэч у тым, што адкрыты ключ, які вам даслаў ваш сябра, неабавязкова дайшоў. Яго можна падмяніць, каб потым чытаць вашую карэспандэнцыю. Таму ключы трэба зьвяраць праз тэлефон ці на асабістай сустрэчы, параўноўваючы іх адбіткі. Калі ўсе словы супадаюць -значыцца, ключ той; калі не супадаюць - ключ падмянілі.



Пара ключоў (key pair) - у PGP ключы ствараюцца толькі парамі: сакрэтны + адкрыты. Вы лёгка зразумееце чаму - калі ўважліва прачыталі, чым адрозьніваюцца сакрэтны й адкрыты ключы.

Рэцыпіент (recipient) - кажучы папросту, тая асоба, для якой вы шыфруеце інфармацыю, атрымальнік, адрасат. Каб зашыфраваць штосьці для пэўнага рэцыпіента, вы мусіце мець ягоны адкрыты ключ. Перачытайце пункт «Адкрыты ключ», калі не разумееце чаму.

Ліставаньне - у кантэксьце PGP - абмен шыфраванымі паведамленьнямі ці файламі. Каб ліставаньне паміж вамі і іншым чалавекам было магчымае, вы мусіце абмяняцца сваімі адкрытымі ключамі (гл. папярэдні пункт).

Подпіс (digital signature) - грае тую ж ролю, што і звычайны рукапісны подпіс: засьведчвае тэкст і любы іншы тып зьвестак, што дазваляе ў далейшым спраўдзіць ці высьветліць паходжаньне інфармацыі.

Подпіс у PGP робіцца сакрэтным ключом, наколькі дзіўна гэта б ні гучала для непадрыхтаванага вуха. Электронны подпіс можа спадарожнічаць шыфроўцы (інфармацыя, зашыфраваная адкрытым ключом рэцыпіента і падпісаная вашым сакрэтным ключом) альбо проста засьведчваць незашыфраваныя зьвесткі. Можа захоўвацца ў асобным файле альбо ў адным з падпісанай інфармацыяй.

PGPTools, PGPKeys - часткі праграмы PGP. Любую зь іх можна запусьціць праз мэню «Пуск» (Start) альбо кляцнуўшы правай кнопкай мышкі на замочак, які PGP, па ўсталяваньні, разьмяшчае каля гадзіньніка, у правым ніжнім куце экрану.

Лякальная кампутаровая сетка і праца ў Інтэрнэце, вірусы і траяны

Падключэньне да Інтэрнэту вашага кампутара дае ворагам неблагія шанцы для выкраданьня інфармацыі. Па-першае, у вас можа быць

незаўважна ўсталяваная праграма-шпег, закінутая вам у выглядзе вірусу ці траяну і, ледзь толькі вы ўвойдзеце ў Сусьветнае павуціньне, яна пачне перасылаць інфармацыю з вашага дыска зламысьнікам. Па-другое, сама апэрацыйная сыстэма можа мець «дзіркі» і памылкі, якія даюць магчымасьць нягоднікам кіраваць вашым кампутарам праз Інтэрнэт (асабліва гэтым «славіцца» Windows, якая найбольш распаўсюджаная ў нашай краіне).

Такім чынам, карыстаньне Інтэрнэтам дапушчальнае толькі ў тым выпадку, калі вы ўсталюеце сабе праграму-фаервол (анг. firewall) ды антывірус.

Фаервол - гэта праграмны сродак, які блякуе недазволеныя сеткавыя апэрацыі, перашкаджаючы шкодным праграмам высылаць штосьці ў Інтэрнэт і зачыняючы доступ да вашага кампутара звонку (з Інтэрнэту). Для карыстальнікаў Windows можна парэкамэндаваць Norton Internet Security, які да таго ж можна ўсталяваць у пары з Norton Antivirus. Людзі ж, якія працуюць з Unix-падобнымі апэрацыйнымі сыстэмамі, збольшага ўратаваныя ад праблемаў зь вірусамі, а фаервол маюць адпачатку (магчыма, яго трэба ўключыць). У Windows XP таксама ёсьць убудаваны фаервол (брандмаўэр), аднак многія людзі не давяраюць ягонай надзейнасьці.

Трэба зазначыць, што абарончае праграмнае забесьпячэньне вымагае наладкі, і вам неабходна будзе паглыбіцца ў вывучэньне суправаджальнай дакумэнтацыі альбо скарыстацца з паслугаў чалавека, якому вы давяраеце.



У выпадку зь лякальнай сеткай лічыцца больш надзейным той кампутар, які непасрэдна падлучаны да Інтэрнэту, ускласьці абавязкі выключна фаерволу і шлюза (разьмеркавальніка Інтэрнэту для іншых кампутараў сеткі) і не працаваць на ім з канфідэнцыйнай інфармацыяй.

Калі ў вашай лякальнай сетцы працуюць людзі, якія не ўваходзяць у кола даверу, пажадана не адкрываць сеткавы доступ да тых дыскаў і каталёгаў, што зьмяшчаюць сакрэтную інфармацыю, альбо, прынамсі, абараняць іх паролем.

Павінна існаваць пісьмова аформленая палітыка бясьпекі ў дачыненьні да кампутараў і сеткі. Усталяваньнем і наладкай праграмаў павінен займацца толькі адзін адказны чалавек - адміністратар сеткі.

Ён абавязаны прытрымлівацца праактыўнага падыходу да патэнцыйных праблемаў: павышаць сваю кваліфікацыю, чытаць электронныя бюлетэні, прысьвечаныя праблемам бясьпекі, рэгулярна абнаўляць апэрацыйную сыстэму, антывірус ды іншыя абарончыя праграмы. Трэба рэгулярна ставіць «заплаткі» на праблемныя месцы ў апэрацыйнай сыстэме і праграмах, што працуюць з Інтэрнэтам.

Праглядні Internet Explorer, усталяваны па змоўчаньні на кожным кампутары з Windows, мае вельмі дрэнную рэпутацыю: цягам доўгага часу ў ім знаходзілі ўсё новыя і новыя дзіркі, якія даюць ліхадзеям магчымасьці для пранікненьня ў ваш кампутар. Пазьбягайце гэтай праграмы! Усталюйце лепш Mozilla Suite ці Mozilla Firefox, што даступныя бясплатна.

Якія існуюць небясьпекі ў захоўваньні кампутаровай інфармацыі?

Небясьпекі ў захоўваньні і перадачы інфармацыі абумоўленыя працоўнымі сытуацыямі. Бясьпека вашай інфармацыі залежыць ад вашага абсталяваньня, вашага праграмнага забесьпячэньня, апэрацыйнай сыстэмы, вашых паводзінаў і парадку ў вашым офісе.

Энэргазахаваньне - таксама праблема бясьпекі. Бальшыня сучасных кампутараў аснаджаныя сыстэмай энэргазахаваньня, якая выключае часткі абсталяваньня, калі пэўны час ніхто не працуе з кампутарам. Пры гэтым зьмесьціва памяці можа быць скінутае на дыск - а ў памяці могуць знаходзіцца дакумэнты, зь якімі вы працуеце.



Зламысьнік можа прасканаваць ваш дыск у пошуку «адбітку памяці», і ёсьць імавернасьць, што яму пашанцуе. Адключыце энэргазахаваньне ў настройках вашай сыстэмы! Зьвярніце ўвагу на тое, што для ноўтбукаў адключэньне можа быць немагчымым альбо можа прывесьці да хуткай разрадкі акумулятараў.

Апэрацыйная сыстэма пэрыядычна скідае кавалкі памяці на дыск у г. зв. «файл падкачкі», каб вызваліць месца

для пэўных патрэбаў. Адпаведна ўзьнікае тая ж небясьпека, што і ў папярэднім пункце, аднак, на шчасьце, у меншым маштабе. Звычайна, адключыць гэтую функцыю, не рызыкуючы стабільнасьцю сыстэмы, немагчыма. TrueCrypt можа аўтаматычна шыфраваць файл падкачкі, але лепш зашыфраваць увесь дыск цалкам.

Ноўтбук - фактар рызыкі. Апроч апісанай вышэй праблемы з энэргазахаваньнем, пераносныя кампутары лягчэй скрасьці, у стомленым стане вы можаце і проста пакінуць яго недзе. Дадамо, што ноўтбук можа быць сканфіскаваны падчас дагляду аўтамабіля ці асабістых рэчаў альбо падчас праезду праз мяжу. Не захоўвайце ў сваім «мабільным офісе» вялікіх масіваў канфідэнцыйнай інфармацыі, захоўвайце толькі тыя рэчы, зь якімі вы зьбіраецеся працаваць бліжэйшым часам. Зразумела, усё павінна быць зашыфраванае.

Небясьпекай выдаленых файлаў. проста выдаліць файл - менш за паўсправы. Сыстэма проста пазначае «месца, занятае гэтым файлам, лічыць свабодным», але нічога не вынішчае.

Адмысловымі сродкамі можна аднавіць файл альбо яго часткі і прачытаць. Замест таго каб выдаляць (анг. delete), файлы трэба вынішчаць (анг. wipe)! Для гэтага выкарыстоўваюцца праграмныя сродкі,напрыклад, Eraser.

Парадак доступу да кампутараў. Чужы чалавек за кампутарам - катастрафічна небясьпечна! Ён можа занесьці вірус альбо выпадкова прачытаць важную інфармацыю, ён можа аказацца аматарам парнаграфіі (і файлы, якія ён пакіне па сябе, скампрамэтуюць вас). І гэта толькі ў тым выпадку, калі ён не зламысьнік.



Калі ж ён мае на мэце шпігоўства - ён можа ўнятрыць у ваш кампутар праграмы, якія перахопяць вашыя паролі і зьвядуць на нуль усю вашую бясьпеку. Дасьведчаны чалавек можа гэта зрабіць, нават калі за ім назіраюць.

Неабходна распрацаваць (пажадана ў пісьмовым выглядзе) парадак доступу да кампутараў. Калі для вас неабходна пускаць іншых людзей папрацаваць на вашыя кампутары, вылучыце адну-дзьве машыны, на якіх будзе адбывацца праца з закрытымі дакумэнтамі, і абмяжуйце да іх доступ.

Асаблівую асьцярожнасьць трэба мець з выкарыстаньнем флэшак,

звычайна на іх «забываецца» інфармацыя. Пажадана іх чысьціць, і не забывацца ў розных месцах.

Узломнікі сыстэмаў карыстаюцца ня толькі тэхнічнымі сродкамі, але і актыўным сацыяльным інжынэрынгам. Вельмі проста - патэлефанаваць і ад чужога імя спытаць нібыта забыты пароль. Часта спрацоўвае. Чытайце біяграфію Кевіна Мітніка, самага «раскручанага» ўзломніка сыстэмаў.

Гіпэртрафія ветлівасьці - крыніца правалаў. Сярэдні беларус, як той японец, ня ўмее казаць цьвёрдага «не».

Прыходзіць, дапрыкладу, у арганізацыю невядомы з чыстым позіркам і, гледзячы проста ў вочы, задае нясьціплыя пытаньні, альбо просіць «на хвілінку» пусьціць да кампутара, альбо імпэтна прапануе свае паслугі ў якасьці добраахвотніка. Выглядае прыстойна, імкнецца гаварыць па-беларуску, на свае паводзіны мае тлумачэньні. Ай, як жа адмовіць, нящетліва ж! Проста дзіва бярэ, як часта гэты - просты ў прынцыпе - фокус спрацоўвае, і людзі сваімі рукамі здаюць канфідэнцыйную інфармацыю.

Іншы варыянт - нахабства. Вы чытаеце важную паперыну ці зьбіраецеся ўвесьці пароль на сваім кампутары, а гэтым часам цераз вашае плячо, не хаваючыся, пачынае пазіраць іншы чалавек. У такой сытуацыі многія людзі няздольныя даць адпор нахабніку і ў выніку «паляць» інфармацыю.



Пераадолець злачынную ветлівасьць дапаможа невялікая доза бюракратыі. Распрацоўвайце правілы, што можна, а чаго нельга. Каму можна сядаць за гэты кампутар, а каму - за гэны. Доступ да дакумэнтаў трэба даваць толькі тым людзям, якія зь імі працуюць. Вызначце, які стаж павінен напрацаваць у вашай арганізацыі чалавек, якія тэсты прайсьці, каб атрымаць свой статус у вашым офісе. Усе правілы павінны быць разьмешчаныя на бачным месцы, каб у іх можна было тыкнуць пальцам. Нават калі некаторыя рэчы падаюцца відавочнымі - усё адно надрукуйце іх ды павесьце на сьцяну. Проста гэта вельмі важны псыхалягічны момант: сказаць камусьці «нельга!» прасьцей, спаслаўшыся на правілы ці загад кіраўніцтва, чым адмовіць «ад сябе». Многія людзі ўвогуле ня ўмеюць адмаўляць, але кожны можа сказаць: «пачытайце правілы, вунь там, на сьцяне» - адмовіўшы такім ускосным чынам.

Як захоўваць папяровыя дакумэнты

Папера - праблема бясьпекі. Звычайна ў офісах няўрадавых арганізацыяў, дзе ёсьць шмат супрацоўнікаў, зьбіраецца шмат дзелавых папераў, якія колісь былі вельмі важныя, а пасьля страцілі сваю актуальнасьць і сталі нікому не патрэбныя - пра іх папросту забыліся. Але для спэцслужбаў і «сэксотаў» яны могуць уяўляць вялікую цікавасьць. Раздрукаваныя паперы з сакрэтнай інфармацыяй (альбо нават і зь несакрэтнай, простай працоўнай інфармацыяй) уяўляюць сабой небясьпеку, якой ня так проста пазбыцца, - героі клясычнай літаратуры палілі дакумэнты ў агні, аднак у наш час такі варыянт малаверагодны, дый паперы стала замнога.



Не выкідайце важныя дакумэнты ў сьметніцу, «органы» могуць наняць пару бамжоў, якія будуць перабіраць сьмецьцевы бак, адбіраючы, апроч пустых пляшак, вашыя паперы. Вынішчайце дакумэнты, у тым ліку і чарнавікі. Просты варыянт - парваць на дробныя кавалкі і высыпаць іх часткамі ў розныя сьметніцы па дарозе дахаты (але і ў гэтым варыянце ня трэба недаацэньваць руплівасьць і апантанасьць некаторых шпегаў-фанатыкаў). Больш зручны і надзейны варыянт - «шрэдэр», здрабняльнік паперы. Гэты апарат наразае паперу на танюткія палосачкі і блытае іх. Аднавіць дакумэнт пасьля гэтага немагчыма.

Адным з небясьпечных момантаў у працы з дакумэнтамі зьяўляецца транспартаваньне дакумэнтаў. Зыходзячы з практыкі, менавіта падчас перамяшчэньня дакумэнтаў і важных папераў гэтыя матэрыялы могуць патрапіць у рукі спэцслужбаў.

Таму перасоўваньне дакумэнтаў у прасторы варта зьвесьці да мінімуму. Замест таго каб паўсюль насіць з сабою важныя дакумэнты, перасоўваючы іх з аднаго “бясьпечнага” месца ў іншае, “яшчэ больш бясьпечнае”, і назад, варта вызначыць сталае месца захоўваньня аль-

бо працы з гэтым дакумэнтам. Тут таксама можна кіравацца прынцыпам дэцэнтралізацыі - можна вызначыць некалькі надзейных месцаў захоўваньня для розных дакумэнтаў. Паверце, што ахранцы будзе цяжэй вызначыць, якая з трыццаці кватэр, якія вы наведалі за тыдзень, будзе вашым “архівам”, чым лавіць вас пастаянна на выхадзе з “палёнай” штаб-кватэры вашай арганізацыі (само памяшканьне штаб-кватэры лепей увогуле пазбавіць будзь-якіх сакрэтных дакумэнтаў).

Ня варта насіць з сабой тыя паперы, якія непатрэбныя вам для дзейнасьці ў дадзены пэрыяд часу. Таксама ня варта захапляцца запаўненьнем нататнікаў важнай інфармацыяй - нататнік у выпадку затрыманьня можа згуляць супраць вас і нават стаць важным рэчавым доказам у крымінальнай справе (падчас аднаго з гучных судовых працэсаў у Беларусі ў якасьці асноўнага доказу супрацьпраўнай дзейнасьці абвінавачанага фігуравала ажно 13 нататнікаў з падрабязнымі зьвесткамі).

Сканфіскаваны нататнік можа выкрыць вашыя кантакты. Таму па магчымасьці інфармацыю ў нататніках варта зьмяшчаць у кадаваным альбо незразумелым для чужога вока выглядзе (самаменш, можна рабіць запісы беларускай лацінкай). Пры запаўненьні нататніка (а таксама пры складаньні іншых дакумэнтаў) было б някепска ўявіць, што гэтыя дакумэнты патрапілі ў рукі спэцслужбаў і тыя іх аналізуюць, - зыходзячы з гэтага можна выправіць тыя моманты, якія зьяўляюцца найбольш небясьпечнымі.



Нататнікі варта мяняць як мага часьцей, пазбаўляючыся ад састарэлых кантактаў і іншай інфармацыі, скарыстаныя нататнікі лепей зьнішчаць, а калі гэта немагчыма - здаваць на часовае захоўваньне ў канспіратыўны “архіў”. У прынцыпе, надзейней усю інфармацыю, якая захоўваецца стала, пераводзіць у лічбавую кадаваную форму.

На дакумэнтах, якія могуць стаць падставай для абвінавачаньня ў зьдзяйсьненьні крымінальнага злачынства (напр. паклёп альбо зьнявага прэзыдэнта, заклікі з мэтай зьвяржэньня канстытуцыйнага ладу ды інш.) варта рабіць прыпіскі, якія б дэзавуявалі сэнс дакумэнту. Напрыклад, на плянах і праграмах можна ставіць надпісы: «Матэрыялы для дэтэктыўнага апавяданьня», «праграма аб’яднаньня “Млада Фронта”, Славаччына, 1929 г.» і г. д. Пад крытычнымі матэрыяламі на адрас прэ-

зыдэнта і дзяржаўнай улады можна ставіць прыпіску: «…але ўсё гэта зьяўляецца няпраўдай і ня мае нічога агульнага з рэчаіснасьцю».

Прынамсі, варта распрацаваць простыя правілы працы з дакумэнтамі для вашай арганізацыі:

- раздрукоўваюцца толькі тыя канфідэнцыйныя дакумэнты, якія раздрукаваць неабходна;
- кожны дакумэнт мусіць мець гаспадара - асобу, якая адказная за яго выраб, працу зь ім і яго зьнішчэньне;
- непатрэбныя дакумэнты зьнішчаюцца ўва ўстаноўленым бясьпечным парадку (гэта датычыцца як канфідэнцыйных дакумэнтаў, так і бягучых дакумэнтаў і чарнавікоў);
- прызначаецца адказны за бясьпеку працы з паперамі.

Як вырабляць, захоўваць і распаўсюджваць друкаваныя матэрыялы

Пры працы з друкаванымі матэрыяламі трэба часава і тэрытарыяльна разьдзяляць фазы вырабу, захоўваньня і распаўсюду. Гэта значыць, што надрукаваны ў друкарні матэрыял не павінен адразу дастаўляцца на штаб-кватэру альбо на кватэру распаўсюднікаў. Пажадана мець кватэру-склад (лецішча, гараж, падсобка), дзе гэтыя матэрыялы будуць захоўвацца ў гуртоўным стане да перадачы на распаўсюд у раздроб. Адначасова на штаб-кватэры павінна быць такая колькасьць друкаваных адзінак, якую не шкада згубіць у выпадку нападу.

Асобы, не заангажаваныя ў выраб друкаванай прадукцыі, не павінны ведаць, дзе знаходзіцца падпольная друкарня. Асобы, якія не займаюцца захоўваньнем друкаванай прадукцыі, не павінны ведаць, дзе знаходзіцца склад улётак. Кожны мусіць ведаць свой участак працы і безь неабходнасьці не цікавіцца, што адбываецца за яго межамі.

Важным і асабліва небясьпечным пытаньнем зьяўляецца транспартаваньне друкаванай прадукцыі - гэтай працай павінны займацца альбо адмысловыя людзі, якія нічым больш не займаюцца, альбо надзейныя, але «незасьвечаныя асобы». На скрайні выпадак транспартаваньнем займаюцца самі актывісты.

Пазьбягайце выкарыстаньня таксовак. Калі няма іншага выйсьця - ускладніце маршрут, мяняйце машыны, кожная новая таксоўка мусіць

быць зь іншай фірмы ці таксапарку, але й нават пры такіх засьцярогах - гэта толькі разавы рэцэпт. Многія кіроўцы таксуюць у адных і тых жа месцах і хутка запомняць незвычайнага пасажыра. Міліцыя і спэцслужбоўцы часта «прачэсваюць» гэтую прафэсійную праслойку, пры гэтым яны могуць выставіць вас у ролі, напрыклад, забойцы ці ліхадзея, так што кожны таксоўца палічыць за абавязак вас «здаць».



Абсалютна недапушчальна транспартаваць незапакаваную ў непразрыстую абгортку прадукцыю - наклад мусіць быць надзейна запакаваны, каб не выклікаць залішніх зачэпак у чужога незацікаўленага вока. У друкарнях часта ставяць на пакункі пазнакі, нярэдка пішуць назвы кніжак. Папрасіце, каб яны не пісалі нічога апроч лічбаў ці ўмоўных знакаў альбо «кодавую назву» (кшталту «Как перестать беспокоиться и начать жить»).

Адкрытыя тэлефонныя размовы пра друкаваную прадукцыю павінны быць выключаныя, а кадаваныя размовы павінны быць зьведзеныя да мінімуму. У выпадку выкарыстаньня кодаў, код трэба рэгулярна мяняць. Безь неабходнасьці ня трэба камунікаваць з падпольнай друкарняй: уладам ня так важна перахапіць канкрэтны наклад улётак, яны хутчэй хочуць увогуле спыніць непадцэнзурны друк на гэтай тэрыторыі. У ідэальным становішчы, рэдакцыя і падпольная друкарня ўвогуле не павінны камунікаваць паміж сабой - мусіць быць адмысловы сувязны, які перадае інфармацыю паміж імі. Таксама ня варта занадта часта камунікаваць праз тэлефон паміж рэзэрвовымі сховішчамі і іншымі элемэнтамі сыстэмы распаўсюду.

Самае горшае, што можна зрабіць, - наладзіць масавую выдачу ўсяго накладу матэрыялаў распаўсюднікам наўпрост на штаб-кватэры: для праваахоўнікаў самае зручнае - зрабіць засаду перад дзьвярыма офісу і перахопліваць распаўсюднікаў. З гэтай жа прычыны распаўсюд трэба пачынаць з тых раёнаў, што знаходзяцца ў далечыні ад штаб-кватэры.



Распаўсюднікі друкаваных матэрыялаў павінны мець пры сабе пасьведчаньне асобы, найлепей пашпарт, ня варта мець пры сабе нічога лішняга. Распаўсюднікі павінны працаваць «у полі» групай (2-5 чалавек) і мець «базу» - г.зн. чалавека, які носіць з сабой вялікую партыю накладу, трымаецца ўбаку ад распаўсюднікаў.

Распаўсюднікі павінны мець пры сабе толькі мінімальную партыю (у

выпадку з пэрыядычнымі выданьнямі - 200-300 асобнікаў), дастатковую для паўгадзіны-гадзіны працы. Калі ў распаўсюднікаў заканчваюцца матэрыялы, яны падыходзяць да «базы» і атрымліваюць новы пачак. Практыка паказвае, што пры дысцыплінаванай працы такі фармат дазваляе зьвесьці да мінімуму колькасьць матэрыялаў, якія трапляюць у лапы мянтам: патрулі, пабачыўшы распаўсюдніка, звычайна адразу імкнуцца схапіць яго. Гэтае правіла датычыцца распаўсюду друкаваных матэрыялаў на вуліцах, у транспарце і шляхам раскідкі па паштовых скрынях.

Калі распаўсюдніка затрымалі і даставілі ў пастарунак, ён не павінен панікаваць і павінен прытрымлівацца загадзя ўзгодненай інструкцыі аб паводзінах падчас затрыманьня. Перад пачаткам працы яму трэба давесьці, што за распаўсюд друкаваных выданьняў прадугледжаны адносна невялікі штраф. Зразумела, ня варта казаць, адкуль узяліся гэтыя друкаваныя матэрыялы (Хто даў? Хто выробляў? Якая арганізацыя займаецца вырабам і распаўсюдам?). Трэба памятаць, што распаўсюднік увогуле можа адмовіцца ад будзь-якіх тлумачэньняў , хоць гэта і патрабуе пэўнай псыхалягічнай загартоўкі.

Таму распаўсюднікі павінны ведаць шэраг шаблонных «адмазак»: «Знайшоў на лаўцы ў сквэры, вырашыў параздаваць сябрам і мінакам» і г. д. Важнае правіла: пасьля затрыманьня нельга адразу ісьці на «базу» альбо штаб-кватэру: існуе небясьпека прывесьці за сабой «хваста».

Асобна адзначым вялікую папулярнасьць і досыць высокую эфэктыўнасьць гэтак званага дэцэнтралізаванага вырабу і распаўсюду друкаваных матэрыялаў. Гэта значыць, напрыклад, што актывістам па ўсёй краіне рассылаюцца праз электронную пошту (альбо зьмяшчаюцца на пэўным сайце ў Інтэрнэце) узоры матэрыялаў, актывісты іх памнажаюць саматужным спосабам (падпольныя друкарні і рызографы тут неабавязковыя, дастаткова хатняй друкаркі альбо партатыўнага ксэракса ў невялічкай арганізацыі) у колькасьці, якая ім неабходная для распаўсюджаньня ўласнымі сіламі. Дзякуючы гэткай тэхналёгіі можна распаўсюдзіць хутка і па ўсёй краіне досыць вялікі наклад. Пры гэтым ня маецца адзінага «цэнтру» вырабу, захоўваньня і распаўсюду, а таксама адсутнічае рызыка, што «тавар» перахопяць пры транспартаваньні.

Пры вырабе і транспартаваньні забароненых кніжак раім выкарыстоўваць дзедаўскую мэтодыку: вокладка кніжкі не павінна

выклікаць аніякіх пытаньняў у «праваахоўнікаў» (кшталту «Самосовершенствование - дорога к успеху»), а пад ёй хаваецца недазволены зьмест (як вы бачыце ў гэтым выданьні). Пазьней «цнатлівую вокладку» можна зьняць.

Пры макетаваньні друкаванай прадукцыі трэба ўлічваць, што беларускае заканадаўства патрабуе разьмяшчэньня на друкаваных вырабах выхадных зьвестак і штрыхавога коду па форме ISBN (штрыхавы код у абавязковым парадку разьмяшчаецца на кнігах і брашурах на чацьвертым баку вокладкі).

Для пэрыядычных выданьняў выхаднымі зьвесткамі лічацца назва выданьня, заснавальнік (заснавальнікі), імя і прозьвішча рэдактара (галоўнага рэдактара альбо ягонага намесьніка), парадкавы нумар выпуску і дата яго выхаду, кошт альбо паметка «Бескаштоўна» ці «Вольны кошт», наклад, поўныя адрасы рэдакцыі і друкарні, рэгістрацыйны нумар.

Па магчымасьці гэтыя зьвесткі павінны разьмяшчацца на пэрыядычным выданьні (нават на тым, якое выдаецца з пазначаным накладам да 300 асобнікаў і не падлягае дзяржаўнай рэгістрацыі). Натуральна, пазначаны наклад усіх незарэгістраваных пэрыядычных выданьняў не павінен перавышаць 300 асобнікаў (гэта значыць, максімум - 299 асобнікаў). Для нелегальных пэрыядычных выданьняў, гэтаксама як і для падпольных кніг і улётак, мае сэнс пазначаць прыдуманыя каардынаты рэдакцыі і друкарні. Цяпер у Беларусі пашыраная практыка, калі выдавец прыдумвае нейкую друкарню з галавы ў нейкім экзатычным расейскім альбо ўкраінскім горадзе ці проста піша «Надрукавана ў Эўропе». Напэўна, тут можна проста цалкам перапісаць каардынаты друкарні зь нейкай расейскай кніжкі.

Як весьці размовы праз тэлефон

Падазрэньне, што спэцслужбы праслухоўваюць усіх, - адно з пашыраных грамадзкіх перакананьняў. Шмат хто лічыць гэта забабонам, спасылаючыся на вялізныя рэсурсы, якіх вымагае гэткая дзейнасьць. На самой справе ў гэтай тэзе шмат што адпавядае рэчаіснасьці, і маштабы праслухоўваньня сапраўды вялікія. Выкрытыя пасьля «памаранчавай рэвалюцыі» ўва Украіне памеры праслухоўваньня тэлефонаў

палітычных і грамадзкіх актывістаў паказваюць, што спэцслужбы не шкадуюць рэсурсаў на гэтую дзейнасьць - слухаюць усіх, чыя дзейнасьць іх цікавіць.

Калі вы карыстаецеся мабільным тэлефонам, то акрамя тэхнічных характэрыстыкаў мадэлі вам нельга забывацца пра чатыры іншыя якасьці гэтага прыстасаваньня: магчымасьць перадачы інфармацыі пра месца знаходжаньня абанэнта; магчымасьць фіксацыі выходных і ўваходных тэлефанаваньняў; магчымасьць праслухоўваньня і запісу размоваў, а таксама SMS'ак; дыстанцыйнае ўключэньне мікрафона для праслухоўваньня нават пры выключаным апараце (апошняе не праверана, але і не абвергнута).



Адзінае галоўнае правіла, якім трэба кіравацца, - **тэлефон не прызначаны для размоваў.** Гэта парадокс павінны быць прынцыпам сакрэтнай дзейнасьці. Калі вам трэба высьветліць нейкае пытаньне, то выкарыстоўвайце тэлефон не для размовы, а для таго, **каб дамовіцца пра час і месца размовы, таксама ў кадаваным выглядзе.** Асабліва гэта правіла датычыцца мабільных тэлефонаў вядомых грамадзкіх актывістаў (некаторыя зь іх кіруюцца правілам «Ну і няхай слухаюць» - і такім чынам даюць спэцслужбам карысную інфармацыю, якая можа быць скарыстаная пазьней ня толькі супраць іх саміх, але і супраць іх карэспандэнтаў).

Лепей дамаўляцца кадаванымі словамі альбо словамі, зразумелымі толькі вам, кшталту «Варыянт С», «Там жа, дзе і пазаўчора», «На прыпынку», «Ля школы», «пад гадзіньнікам». Замест таго каб казаць: «У кавярні “Вавёрачка” - лепей выкарыстаць код альбо сказаць: «У кавярні на партызанскім» ці «Ну, памятаеш, на Мотавела…» Асабліва пільнымі ў гэтым сэнсе трэба быць падчас маштабных акцыяў, важных сустрэчаў і перамоваў, выбарчых і іншых палітычных кампаніяў. SMS-паведамленьні такія ж небясьпечныя, імі таксама трэба абменьвацца асьцярожна, з выкарыстаньнем коду.

Сачыце, каб у памяці вашага мабільніка не было лішніх SMS'ак (на выпадак адабраньня мабільніка).

Памятайце, што спэцслужбы часта зважаюць на колькасьць званкоў з аднаго тэлефона на іншы: напрыклад, калі «пад каўпаком» знаходзіцца апазыцыйны дзяяч, то аўтаматычна зьвяртаецца ўвага на

тыя нумары, на якія ён часьцей за ўсё тэлефануе (з хатняга і мабільнага тэлефона). Напрыклад, калі дзяяч, які знаходзіцца ў прыярытэтным сьпісе праслухоўваньня, патэлефанаваў чалавеку першы раз у жыцьці (нават памыліўся нумарам), то гэты абанэнт аўтаматычна трапляе ў калектыўную памяць органаў і ўжо ня будзе забыты.

Шырока распаўсюджанае меркаваньне пра магчымасьць «захаваць інкогніта», тэлефануючы з таксафонаў, не зьяўляецца 100% праўдзівым.

Першая акалічнасьць: тэлефонная картка мае свой унікальны код (ідэнтыфікатар), які фіксуецца пры выкарыстаньні. Гэта можа даць ліхадзеям багата зьвестак для аналізу. Напрыклад, з адной і той жа карткай перадавалася інфармацыя апазыцыянэру А і рабіліся тэлефанаваньні ў прыватную кватэру Б. Гэта дае падставы меркаваць, што званіў сам Б, альбо хтосьці блізкі да яго. Адсюль выснова: для сапраўды ананімнага тэлефанаваньня выкарыстоўваецца асобная картка, і толькі 1 раз! Скончыўшы размову, забярыце картку, а потым «забудзьцеся» на яе ў іншым таксафоне. Хтосьці падбярэ і сваімі званкамі створыць інфармацыйны шум, заблытваючы патэнцыйных шпегаў.

Другая акалічнасьць: голас кожнага чалавека ўнікальны і паддаецца аналізу ды параўнаньню. Значыцца, калі ваш голас падчас размовы будзе запісаны, то існуе верагоднасьць, што вас «вылічаць». Гэты мэтад усё яшчэ малараспаўсюджаны і дарагі, таму звычайна выкарыстоўваецца ў небанальных сытуацыях, аднак мець гэта на ўвазе трэба. Падкрэсьлім, што спробы зьмяняць свой голас найчасьцей не дапамагаюць, за выняткам сытуацый, калі выкарыстоўваюцца спэцыяльныя электронныя прыстасаваньні для скажэньня голасу.



Падчас канфідэнцыйных і важных размоваў мабільны тэлефон трэба адключаць і вымаць батарэю (найлепей зрабіць гэта загадзя, ня ў тым месцы, дзе адбываюцца перамовы). Заўжды добра, калі вы ня возьмеце з сабою тэлефона, калі пойдзеце на сустрэчу: памятайце, што праз мабільны тэлефон нескладана вылічыць вашае месца знаходжаньня (дакладнасьць можа быць высокай: ажно да нумару дому). пакіньце мабільнік у офісе ці дома (адключаным альбо ўключаным) - і ідзіце на сустрэчу. Калі вам асабліва каштоўная канфідэнцыйнасьць - па-магчымасьці рэгіструйце мабільныя тэлефоны на іншых, незасьвечаных асобаў (а таксама можна карыстац-

ца карткамі замежных апэратараў з роўмінгам). Але ўлічвайце, што ў мабільных сетках рэгіструецца ня толькі SIM-картка, але й тэлефонны апарат,- таму для новых і замежных SIM-картак лепей выкарыстоўваць новыя апараты. Практычная заўвага: калі батарэі вашага тэлефона звычайна хапала на пяць дзён размоваў, а раптам яна стала разраджацца за дзень - верагодна, што ў вашым тэлефоне працуе «жучок», хаця, магчыма, проста прыйшоў час замяніць акумулятар.

Існуюць прылады, прызначаныя для зьнішчэньня альбо выяўленьня «жучкоў» у памяшканьнях, аўтамабілях, на тэлефонных ды электрадратах. Яны, на жаль, каштуюць немалых грошай і вымагаюць досьведу, якога ў вас хутчэй за ўсё няма.

Апроч таго, у гэтай сфэры ўсё імкліва разьвіваецца, так што, калі ў вас няма свайго (вартага даверу) адмыслоўцы, то лепш проста не абгаворвайце сакрэтных справаў у «папаленых» памяшканьнях. Ня трэба ствараць сталых месцаў для перамоваў, улічвайце, што кавярні і рэстарацыі - зручныя для праслухоўваньня месцы, у якіх (хаця б і выпадкова) могуць аказацца варожыя вушы.

Пераезд праз мяжу



Лепей устрымацца ад перавозу праз мяжу канфідэнцыйных, сакрэтных і проста важных дакумэнтаў, а таксама буйных сумаў наяўных грошаў. Калі гэтага нельга пазьбегнуць, то дакумэнты варта правозіць у выглядзе зашыфраванай электроннай вэрсіі (гл. заўвагі пра рэзэрвовыя копіі). Майце на ўвазе, што мытнікі маюць тэхнічныя магчымасьці для прагляду электронных носьбітаў. Тэарэтычна, яны могуць не прапусьціць яўна зашыфраваную інфармацыю. Абавязкова трэба карыстацца крыптаграфіяй (шыфраваньнем), а найлепей, каб не выклікаць залішніх падазрэньняў, - стэганаграфіяй (гл. вышэй).

Можна адзначыць, што ў мабільнікі, аснаджаныя такімі функцыямі, як інфрачырвоны порт альбо bluetooth, у прынцыпе, можна запісаць ня толькі мэлёдыю альбо застаўку, але й любы файл (прынамсі, для многіх мадэляў). Памер файлу абмежаваны свабоднай памяцьцю тэлефона, але можа аказацца дастатковым для некаторых дакумэнтаў (зразумела ж, у зашыфраваным выглядзе). Загадзя прадумайце, як вы будзеце «даставаць» файл з свайго сотавага сябра, для гэтага: 1) у тэлефоне мусіць быць функцыя «выслаць праз інфрачырвоны порт (альбо bluetooth)»; 2) спатрэбіцца кампутар, здольны прымаць файлы праз той жа порт (сучасныя ноўтбукі звычайна гэта могуць).

Надзейнасьць такога спосабу яшчэ вымагае ацэнкі. У прынцыпе, амаль у любы мабільны тэлефон можна закачаць пэўную колькасьць інфармацыі з дапамогай камунікацыйнага кабелю. А яшчэ зручней для перавозу інфармацыі праз мяжу карыстацца mp3-плэерамі і лічбавымі фотаапаратамі, якія абсалютна легальна могуць утрымліваць некалькі соцень мегабайтаў альбо нават гігабайтаў інфармацыі і не выклікаюць залішніх падазрэньняў. Для староньняга вока гэта проста плэер (яго і слухаць трэба, а ня толькі інфармацыю праз мяжу вазіць) альбо звычайны фотаапарта (колькі іх перасякае мяжу за дзень!).



Беларускае заканадаўства дазваляе ўвозіць у краіну без дэкляраваньня суму, эквівалентную 10 000 даляраў ЗША, але калі сума большая, то яна падлягае абавязковаму дэкляраваньню. Паходжаньне грошай пазначаць ня трэба. Трэба, аднак, ведаць, што зьвесткі пра дэкляраваньне потым трапляюць у падатковую інспэкцыю і розныя правяраючыя органы, таму пазьней тыя могуць пачаць расьсьледаваньне - што гэта за грошы, ці сплачаныя зь іх падаткі? Але пры перасячэньні мяжы ніякіх дакумэнтаў ня трэба. Што тычыцца расейска-беларускай мяжы, дык праз яе дазволена правозіць любую колькасьць валюты без аніякага дэкляраваньня. Аднак на іншых межах недэкляраваныя грошы, па-першае, канфіскуюць, па-другое, могуць нават распачаць крымінальную справу аб кантрабандзе. Пры дэкляраваньні грошай ні ў якім разе нельга пазначаць, што яны вязуцца для мэтаў няўрадавай арганізацыі (бяз розьніцы, зарэгістраванай альбо незарэгістраванай) альбо дзеля мэтаў гуманітарнае дапамогі.

Не забывайцеся, што ў Беларусі існуе некалькі ступеняў кантролю за перасоўваньнем грамадзянаў праз мяжу.

Існуе сьпіс асобаў, перасоўваньне якіх празь мяжу адсочваецца, а ў дачыненьні да некаторых асобаў стала выкарыстоўваецца асабісты дагляд (асобы, якія перасякаюць мяжу разам з гэтымі людзьмі, таксама трапляюць у кантрольны сьпіс). Таму без асаблівай неабходнасьці ня варта афішаваць на мяжы сваю датычнасьць да вядомых дзеячоў, да якіх скіраваная пільная ўвага памежнікаў і мытнікаў.

На мяжы мытнікі маюць права правесьці ня толькі дагляд рэчаў, але і асабісты дагляд, і дагляд транспартнага сродку. У выпадку, калі ў транспартным сродку будзе знойдзеная будзь-якая кантрабанда, нават калі гэта цыгарэты ці піва, транспартны сродак можа быць сканфіскаваны. Асабісты дагляд можа выкарыстоўвацца толькі на асабісты загад начальніка мытнага паста.

Асабісты дагляд патрабуе складаньня пратаколу дагляду і павінны адбывацца ў спэцыяльна прыстасаваным памяшканьні ў прысутнасьці панятых таго ж полу, што і вы. Калі вы ня маеце пры сабе анічога крамольнага і вам прапануюць прайсьці асабісты дагляд - не лянуйцеся, патрабуйце выкананьня ўсіх фармальнасьцяў працэдуры, гэтым вы можаце дапамагчы іншым людзям.

частка

B

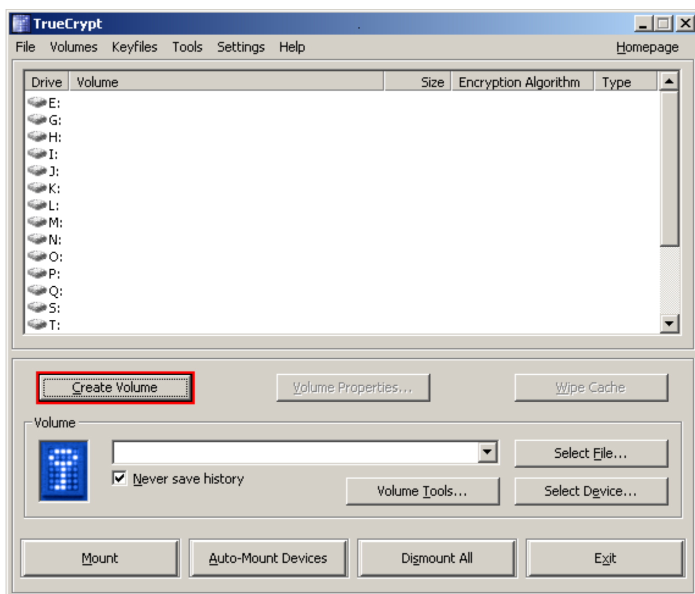
Як стварыць і як карыстацца TrueCrypt кантэйнерам?

Як стварыць і як карыстацца TrueCrypt кантэйнэрам?

У гэтай частцы вы знойдзеце пакрокавую інструкцыю як стварыць, змантаваць TrueCrypt том, і як ім карыстацца. Мы настойліва рэкамендуем вам таксама азнаёміцца зь іншымі разьдзеламі гэтага даведніка, бо яны зьмяшчаюць важную інфармацыю.

Крок 1:

Калі вы гэтага яшчэ не зрабілі, то запампуйце і ўсталюйце TrueCrypt. Запусціце TrueCrypt: двойчы пстрыкніце па файлу TrueCrypt.exe альбо па ярлыку TrueCrypt у меню Windows “Пуск”.



Крок 2:

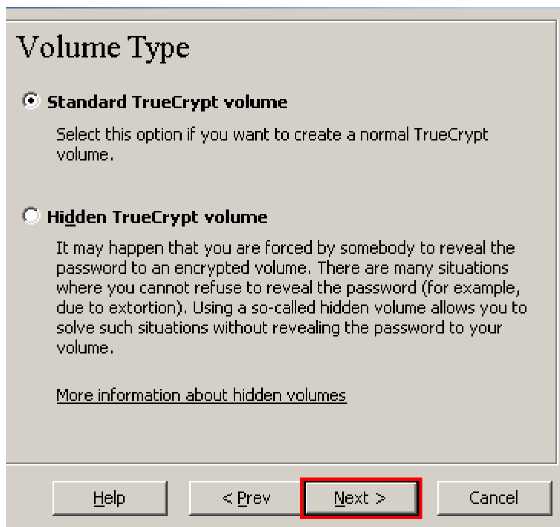
TrueCrypt GUI (Graphical user interface)

Павінна зьявіцца галоўнае вакно TrueCrypt. Пстрыкніце “Create Volume” (вылучана чырвоным прастакутнікам).

Крок 3:
TrueCrypt GUI
Павінна зьявіцца вакно майстра стварэньня тамоў TrueCrypt.



Тут вы павінны выбраць, дзе хочаце стварыць том TrueCrypt. Том TrueCrypt можа захоўвацца ў файле, які таксама завецца кантэйнэр, на разьдзеле жорсткага дыску альбо на назапашвальніку. У гэтым дапаможніку мы абярэм першы варыянт і створым том TrueCrypt у файле.



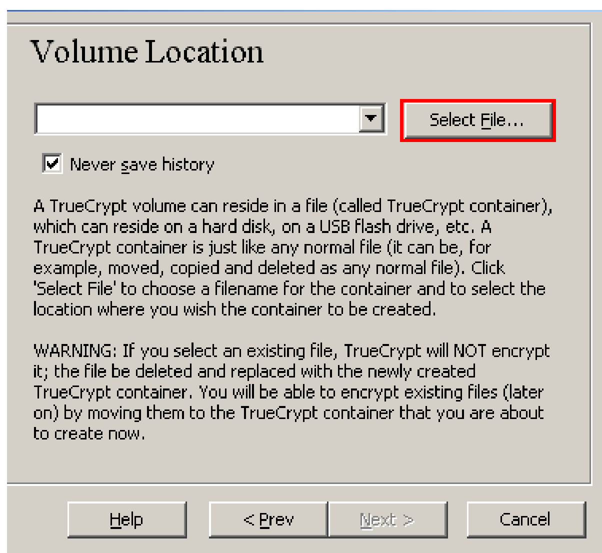
Гэтая опцыя стаіць па змаўчаньні, таму вы проста можаце пстрыкнуць “Next”.

Заўвага: на наступных кроках скрыншоты будуць адлюстроўваць толькі правую частку вакна майстра стварэньня.

Крок 4:

TrueCrypt GUI

Тут вы павінны выбраць, які том TrueCrypt вы хочаце стварыць: стандартны альбо схаваны.



У гэтым дапаможніку мы абярэм першую опцыю і створым стандартны том TrueCrypt.

Гэтая опцыя стаіць па змаўчаньні, таму вы проста можаце пстрыкнуць “Next”.

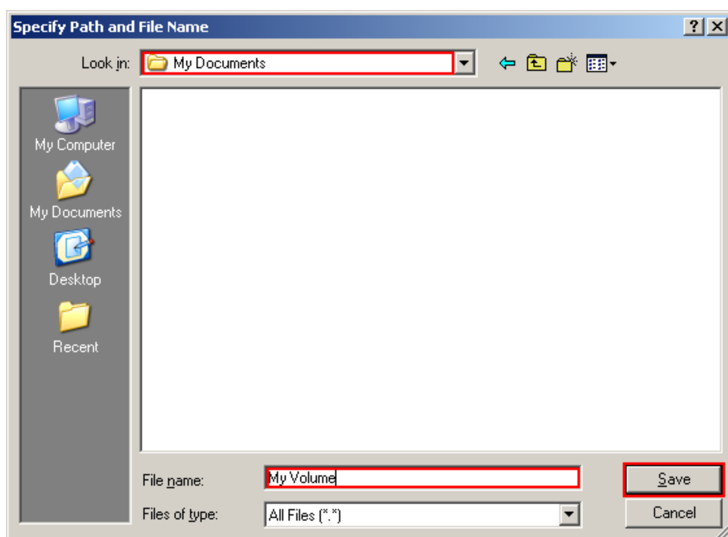
Крок 5:

TrueCrypt GUI

Тут вы павінны вызначыць, дзе хочаце стварыць том TrueCrypt (файлавы кантэйнэр). Майце на ўвазе, што кантэйнэр TrueCrypt працуе як любы звычайны файл. Яго можна, напрыклад, перамясьціць альбо выдаліць як любы звычайны файл. Яму таксама патрэбнае файлавае імя, якое вы абярэце на наступным кроку.

Пстрыкніце “Select File”.

Зьявіцца стандартная панэль выбару файлаў Windows (пры гэтым



вакно майстра стварэньня тамоў TrueCrypt застанецца адчыненым на заднім плане).

Крок 6:

Панэль выбару файлаў

У гэтым дапаможніку мы створым наш том TrueCrypt у тэчцы D:\My Documents\, і файлавае імя тома (кантэйнэра) будзе My Volume (як вы бачыце на скрыншоце ніжэй). Зразумела, вы можаце абраць іншае імя файла і месцазнаходжаньне (напрыклад, USB картку памяці). Заўважце, што пакуль яшчэ не існуе файла з назвай My Volume, TrueCrypt яго створыць.

ВАЖНА: Майце на ўвазе, што TrueCrypt не шыфруе ўжо існуючыя файлы (падчас стварэньня файлавага кантэйнэра TrueCrypt). Калі на гэтым кроке вы абярэце ўжо існуючы файл, ён будзе перазапісаны і заменены на новаствораны том (гэта значыць, што перазапісаны файл проста згубіцца, а не зашыфруецца). Пазней вы зможаце зашыфраваць ужо існуючыя файлы, калі перамясьціце іх у том TrueCrypt, які мы зараз ствараем.*

Абярыце жаданы маршрут (дзе вы хочаце стварыць кантэйнэр) на панэлі выбару файлаў.

Надрукуйце імя файла, якое вы жадаеце, у панэлі імені файла.

Пстрыкніце “Save”.

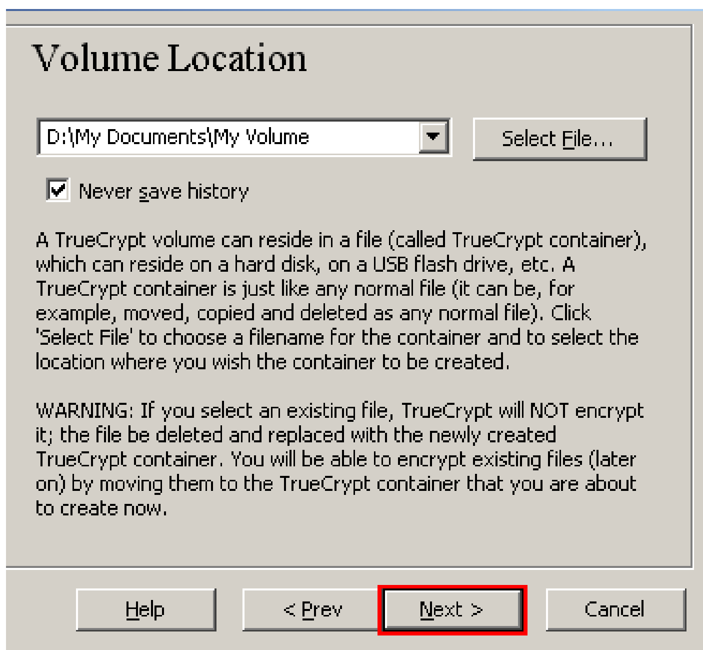
Панэль выбару файлаў павінна зьнікнуць.

На наступных кроках мы вернемся да майстра стварэньня тамоў TrueCrypt.

*Майце на ўвазе, што пасля таго, як вы скапіявалі існуючыя незашыфраваныя файлы ў том TrueCrypt, вам трэба бясьпечна выдаліць арыгіналы незашыфраваных файлаў.

Існуюць розныя інструмэнтальныя сродкі, якія дазваляюць бясьпечна выдаляць файлы (многія зь іх бясплатныя).

Крок 7:
TrueCrypt GUI

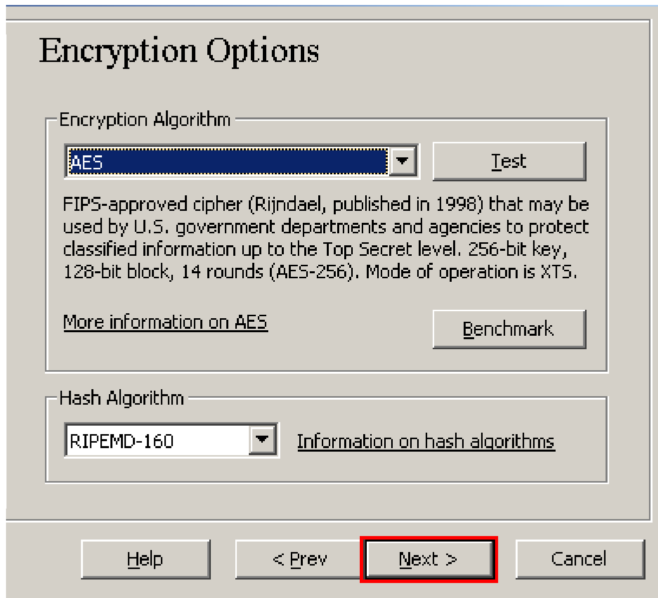


У вакне майстра стварэньня тамоў пстрыкніце “Next”.

Крок 8:

TrueCrypt GUI

Тут вы можаце абраць альгарытм шыфраваньня і алгарытм хэшыраваньня для тому.



Калі вы ня ўпэўнены, што абраць, вы можаце пакінуць налады па змаўчаньні і пстрыкнуць “Next” (калі вам патрэбная больш дэталёвая інфармацыя, глядзіце разьдзелы “Альгарытмы шыфраваньня” і “Альгарытмы хэшыраваньня”).

Крок 9:

TrueCrypt GUI

Тут мы ўдакладняем, што хочам, каб памер нашага TrueCrypt кантэйнэру быў 1 Мегабайт. Вы, зразумела, можаце абраць іншы памер. Пасьля таго, як вы надрукавалі пажаданы памер у полі ўвода (вылучана чырвоным прастакутнікам), пстрыкніце “Next”.

Крок 10:

TrueCrypt GUI

Гэта адзін з найважнейшых крокаў. Тут вы павінны абраць добры пароль для тома.

Уважліва азнаёмцеся з інфармацыяй, прадстаўленай у вакне майстра стварэння тамоў, наконт таго, які пароль лічыцца добрым.

Volume Password

Password:

Confirm:

Display password

Use keyfiles

Keyfiles...

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.

Help | < Prev | Next > | Cancel

Пасьля таго, як вы абралі добры пароль, надрукуйце яго ў першым полі ўвода. Пасля надрукуйце яго яшчэ раз у другім полі ўвода, які знаходзіцца пад першым, і пстрыкніце “Next”.

Заўвага: кнопка “Next” ня будзе працаваць, пакуль паролі ў абодвух палях увода ня будуць супадаць.

Крок 11:

TrueCrypt GUI

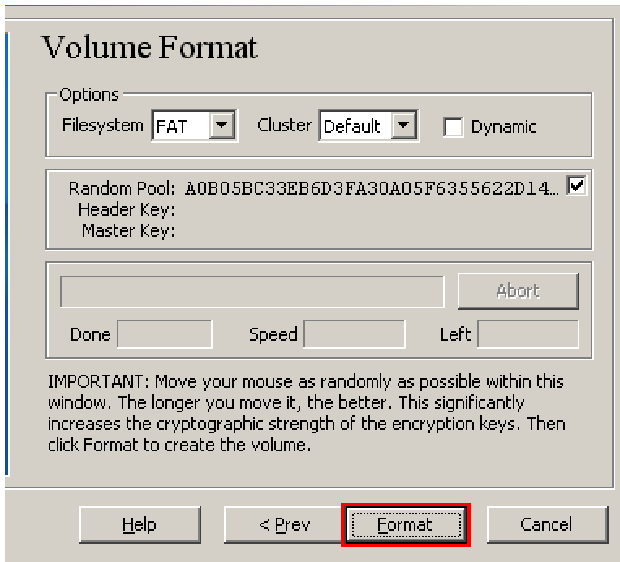
Павадзіце мышкай па вакну майстра стварэньня тамоў настолькі бязладна, наколькі магчыма, як мінімум 30 секунд.

Чым даўжэй вы будзеце рухаць мышкай, тым лепш. Гэта значна павялічвае крыптаграфічную моц ключоў шыфраваньня (што павялічвае бяспеку).

Пстрыкніце “Format”.

Павінна распачацца стварэньне тома. TrueCrypt зараз створыць файл пад назвай My Volume у тэчцы D:\My Documents\ (як мы адзначылі на

кроку 6). Гэты файл будзе TrueCrypt кантэйнэрам (у ім будзе зьмяшчацца зашыфраваны том TrueCrypt).

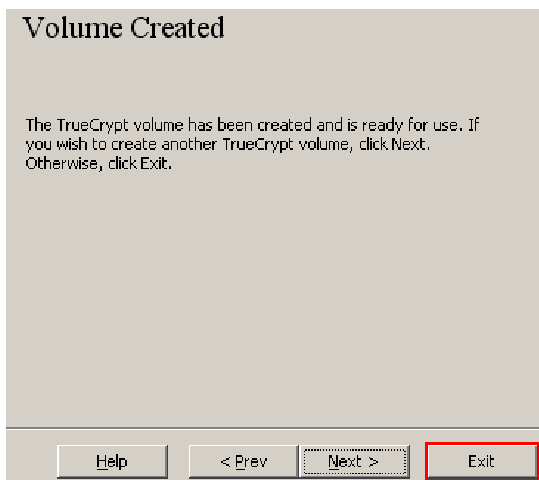


Стварэньне тому можа заняць і працяглы час, гэта залежыць ад памеру тома. Пасля таго як стварэньне тому скончыцца, зьявіцца наступнае дыялёгавае вакно:



TrueCrypt GUI
Пстрыкніце “OK”, каб зачыніць дыялёгавае вакно.

Крок 12:
TrueCrypt GUI
Мы толькі што пасьпяхова стварылі том TrueCrypt (файлавы кантэйнэр). У вакне майстра стварэньня тамоў TrueCrypt пстрыкніце “Exit”.



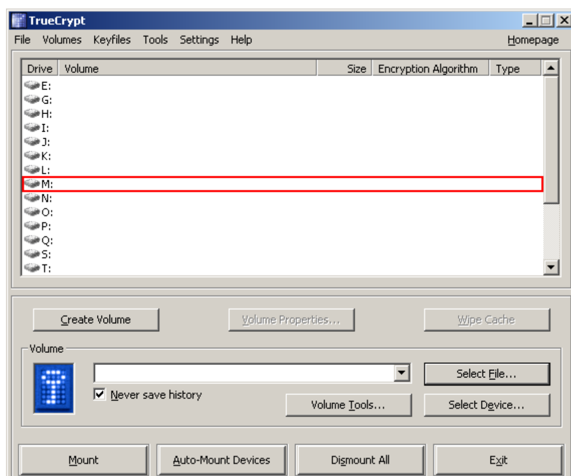
Вакно майстра стварэньня павінна зьнікнуць.

На наступных кроках мы будзем мантаваць том, які толькі што стварылі. Мы вяртаемся да галоўнага вакна TrueCrypt (якое павінна быць яшчэ адчынена, але калі не, то паўтарыце крок 1, каб запусціць TrueCrypt, а пасля працягвайце, пачынаючы з кроку 13).

Крок 13:

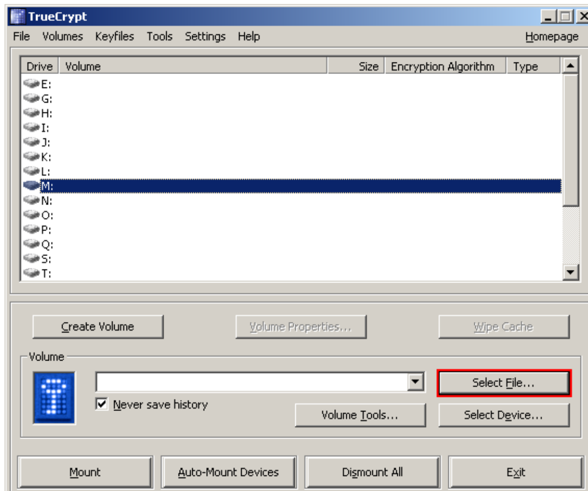
TrueCrypt GUI

Абярыце імя дыску са сьпісу (вылучана чырвоным прастакутнікам). Гэта будзе імя дыску, да якога кантэйнэр TrueCrypt будзе змантаваны.

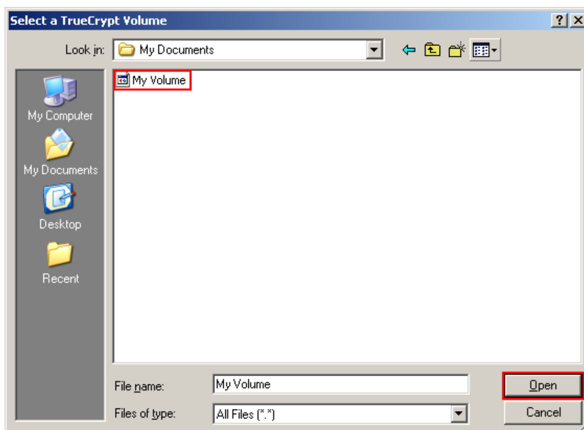


ЗАЎВАГА: У гэтым дапаможніку мы абярэм **імя дыску M,** але вы, зразумела, можаце абраць любое іншае даступнае імя дыску.

Крок 14:
TrueCrypt GUI
Пстрыкніце “Select File”.
Павінна зьявіцца стандартная панэль выбару файлаў.



Крок 15:
Панэль выбару файлаў



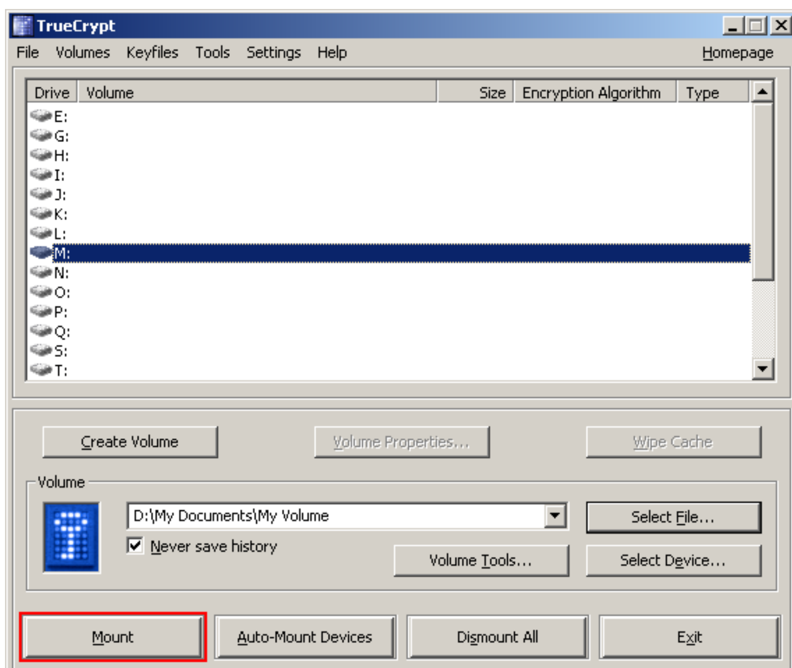
У гэтай панэлі выбару файлаў знайдзіце файлавы кантэйнэр (які мы стварылі на кроках 6-11) і абярыце яго.

Пстрыкніце “Open” (у вакне панэлі выбару файлаў).

Вакно панэлі выбару файлаў павінна зьнікнуць.

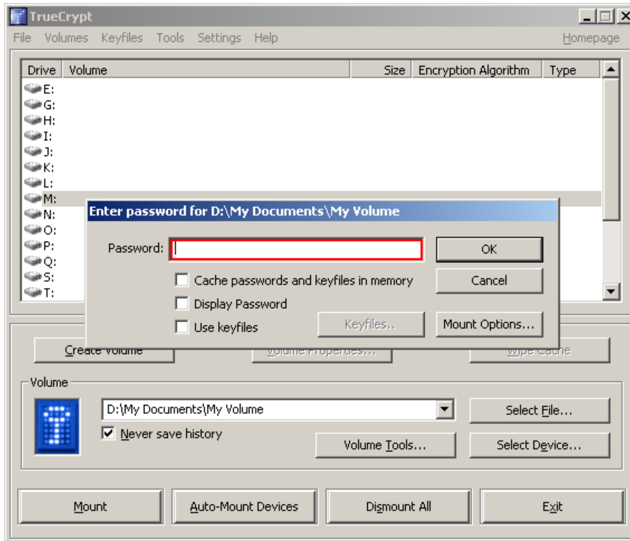
На наступных кроках мы вернемся да галоўнага вакна TrueCrypt.

Крок 16:
TrueCrypt GUI
У галоўным вакне TrueCrypt пстрыкніце “Mount”.



Павінна зьявіцца дыялёгавае вакно для ўвядзеньня паролю.

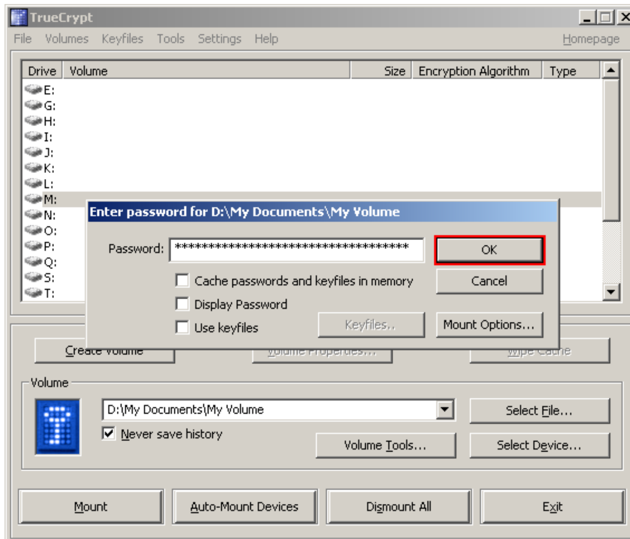
Крок 17:
TrueCrypt GUI
Надрукуйце пароль (які вы указалі на кроку 10) у полі ўводу пароля (вылучана чырвоным простакутнікам).



Крок 18:

TrueCrypt GUI

Пстрыкніце “OK” у вакне для ўвядзеньня паролю.



Зараз TrueCrypt паспрабуе змантаваць том. Калі пароль няправільны

(напрыклад, калі вы няправільна яго надрукавалі), TrueCrypt вам паведаміць, і вам патрэбна будзе тады паўтарыць папярэдні крок (зноў надрукаваць пароль і пстрыкнуць “OK”). Калі пароль правільны, том будзе змантаваны.

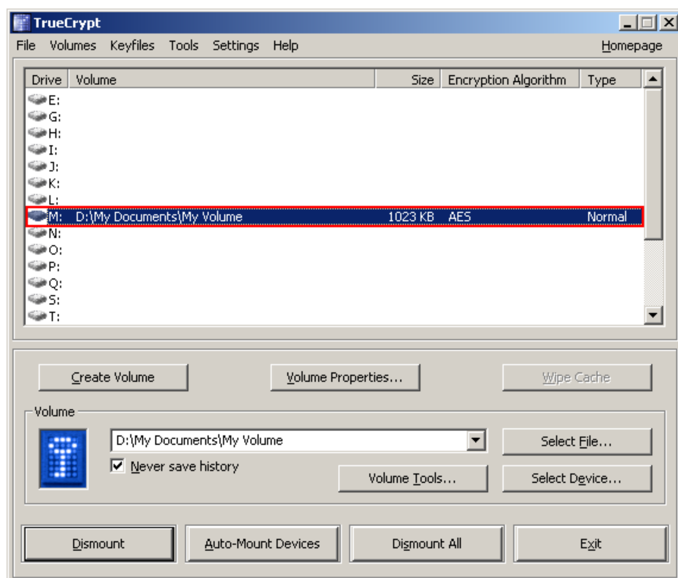
Апошні крок:

TrueCrypt GUI

Мы толькі што пасьпяхова змантавалі кантэйнэр як віртуальны дыск M:

Віртуальны дыск цалкам зашыфраваны (уключаючы імёны файлаў, табліцы разьмяшчэньня файлаў, свабодную прастору і гэтак далей) і паводзіць сябе як звычайны дыск.

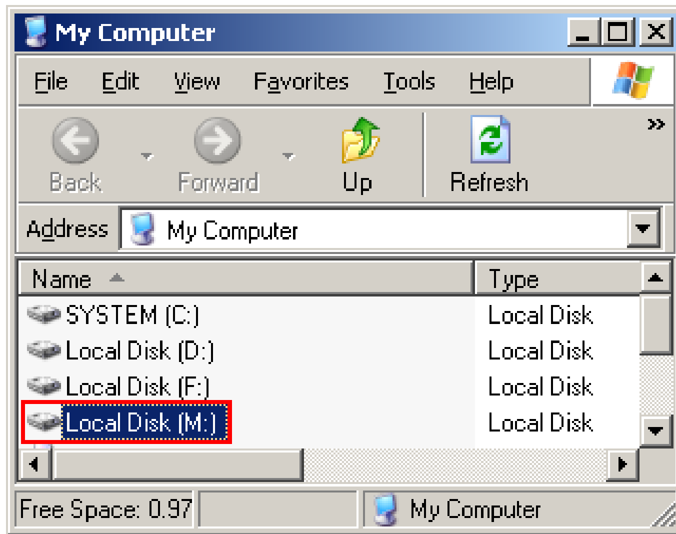
Вы можаце захоўваць файлы (альбо капіяваць, перамяшчаць і г.д.) на гэтым віртуальным дыске, і яны будуць шыфравацца адразу падчас іх запісваньня.



Калі вы адчыняеце файл, які захоўваецца ў томе TrueCrypt, напрыклад, у мэдыяплэеры, файл аўтаматычна расшыфроўваецца ў АЗП (памяці) адразу падчас загрузкі.

ВАЖНА: Майце на ўвазе, што калі вы адчыняеце файл, які захоўваецца

ў томе TrueCrypt (альбо калі вы запісваеце/капіюеце файл з/на том TrueCrypt), у вас ня будзе зноў запытвацца пароль. Вам трэба будзе ўвесьці правільны пароль толькі падчас змантаваньня тому.



Вы можаце адчыніць змантаваны том, напрыклад, двойчы пстрыкнуўшы па пункце, вылучаным чырвоным прастакутнікам, як паказана на скрыншоце вышэй.

Вы можаце адчыняць змантаваны том такім чынам, як вы звычайна адчыняеце любыя іншыя віды тамоў.

Напрыклад, адчыняеце сьпіс “Кампутар” (альбо “Мой кампутар”) і двойчы пстрыкаеце на адпаведнае імя дыску (у дадзеным выпадку гэта дыск M).

Сьпіс “Мой кампутар”

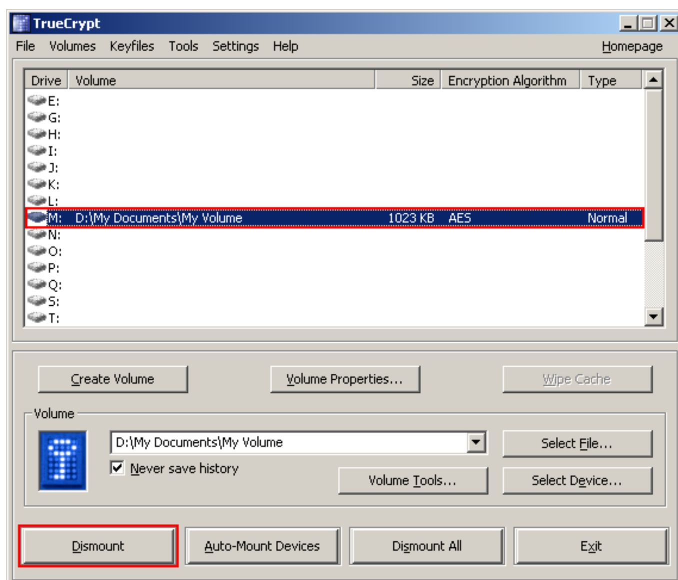
Вы можаце капіяваць файлы (альбо тэчкі) зь / і на том TrueCrypt такім жа чынам, як вы гэта робіце з любым звычайным дыскам (напрыклад, прастымі апэрацыямі пацягнуць і пакінуць). Файлы, якія счытваюцца альбо капіююцца з тома TrueCrypt адразу аўтаматычна расшыфроўваюцца ў АЗП (памяці).

Такім жа чынам файлы, якія запісваюцца альбо капіююцца на том TrueCrypt, адразу аўтаматычна шыфруюцца ў АЗП (як раз перад тым, як запісацца на дыск).

МАЙЦЕ НА ЎВАЗЕ, што TrueCrypt ніколі не захоўвае расшыфраваныя дадзеныя на дыск, ён толькі часова разьмяшчае іх у АЗП (памяці). Нават калі том змантаваны, дадзеныя, якія ў ім захоўваюцца, усё адно зашыфраваныя.

Калі вы перазагрузіце Windows альбо выключыце кампутар, том размантуецца і ўсе файлы, якія на ім захоўваюцца, будуць недаступны (і зашыфраваны). Нават калі электрасілкаваньне раптоўна зьнікне, і вы не паспееце належным чынам зачыніць сыстэму, усе файлы, якія захоўваюцца ў томе, будуць недасягальнымі (і зашыфраванымі). Каб зрабіць іх даступнымі зноў, вам патрэбна будзе змантаваць том. Каб гэта зрабіць, паўтарыце крокі 13-18.

Калі вы хочаце зачыніць том і зрабіць файлы, захаваныя на ім, недаступнымі, альбо перазапусьціце апэрацыйную сыстэму, альбо размантуйце том. Каб гэта зрабіць, зрабіце наступныя крокі:



TrueCrypt GUI

Абярыце том са сьпісу змантаваных тамоў у галоўным вакне TrueCrypt (вылучана чырвоным прастакутнікам на скрыншоце вышэй) і пстрыкніце “Dismount” (таксама вылучана чырвоным прастакутнікам на скрыншоце вышэй). Каб зрабіць файлы, захаваныя на ім, даступнымі

зноў, вам трэба будзе змантаваць том. Каб гэта зрабіць, паўтарыце крокі 13-18.

Як стварыць і як карыстацца разьдзелам/прыладай, зашыфраванымі TrueCrypt?

Замест таго, каб ствараць файлавыя кантэйнэры, вы таксама можаце шыфраваць фізычныя разьдзелы альбо назапашвальнікі (гэта значыць ствараць тамы TrueCrypt на базе прыладаў). Каб гэта зрабіць, паўтарыце крокі 1-3, але на кроке 3 абярыце другую альбо трэцюю опцыю.

Пасьля прытрымлівайцеся інструкцыі майстра стварэньня тамоў. Калі вы ствараеце том TrueCrypt на базе несыстэмнага разьдзела альбо назапашвальніка, вы можаце змантаваць яго, пстрыкнуў “Auto-Mount Devices” у галоўным вакне TrueCrypt. Інфармацыю па шыфраваньні сыстэмных разьдзелаў/назапашвальнікаў вы можаце знайсці ў разьдзеле “Шыфраваньне сыстэмы”.

ВАЖНА: мы настойліва рэкамэндуем азнаёміцца зь іншымі разьдзеламі даведніка, бо ў іх зьмяшчаецца важная інфармацыя, якую мы апусьцілі ў гэтым дапаможніку дзеля прастаты.

Шыфраваньне апэрацыйнай сыстэмы

TrueCrypt можа на ляту шыфраваць сыстэмны падзел ці ўвесь сыстэмны дыск, то бок падзел ці дыск, на якім усталяваная апэрацыйная сыстэма і зь якога яна запускаецца.

Шыфраваньне сыстэмы дае высокі ўзровень бясьпекі і прыватнасьці, таму што ўсе файлы, у тым ліку часовыя, якія Windows і прыкладаньні ствараюць на сыстэмным падзеле (як правіла, бяз вашага ведама і згоды), файлы гібернацыі, файлы падпампоўкі і г.д., заўсёды зашыфраваныя (нават калі сілкаваньне раптам перарываецца). Windows таксама запісвае вялікія аб'ёмы патэнцыйна ўразьлівых дадзеных, напрыклад, назовы й месцазнаходжанне файлаў, якія адкрываліся, прыкладаньняў, якія Вы запускалі і г.д. Усе файлы рэгістрацыі і запісы рэестру таксама заўжды зашыфроўваюцца.

Шыфраваньне сыстэмы ўключае ў сябе аўтарызацыю перад запускам. Гэта азначае, што любы, хто хоча атрымаць доступ да шыфраванай сыстэмы і карыстацца ёй, напрыклад, чытаць і запісваць файлы, якія захоўваюцца на сыстэмным дыску, мусіць увесьці правільны пароль перад кожнай загрузкай Windows. Аўтарызацыю перад загрузкай ажыцьцяўляе TrueCrypt Boot Loader, які знаходзіцца ў першым запісе загрузнага дыска і на дыску аднаўленьня TrueCrypt.

Заўважце, што TrueCrypt можа зашыфраваць існуючы нешыфраваны сыстэмны падзел ці дыск падчас працы апэрацыйнай сыстэмы (т.б. калі сыстэма зашыфроўваецца, вы можаце карыстацца кампутарам як звычайна, безь якіх-небудзь абмежаваньняў). Таксама, зашыфраваны сыстэмны падзел ці дыск можа быць расшыфраваны падчас працы апэрацыйнай сыстэмы. Вы ў любы час можаце перапыніць працэс шыфраваньня або дэшыфраваньня, пакінуць падзел ці дыск часткова зашыфраваным, перазагрузіць або выключыць кампутар, а затым аднавіць працэс, які будзе працягнуты з моманту яго спыненьня.

Каб зашыфраваць сыстэмны падзел ці ўвесь сыстэмны дыск, выберыце System > Encrypt System Partition/Drive і кіруйцеся інструкцыямі майстра. Каб расшыфраваць сыстэмны падзел ці дыск, выберыце System > Permanently Decrypt System Partition/Drive.

Для шыфраваньня сыстэмы выкарыстоўваецца рэжым працы XTS (гл. разьдзел “Рэжымы працы”). Тэхнічныя падрабязнасьці шыфраваньня сыстэмы апісаныя ў разьдзеле “Схема шыфраваньня” ў главе “Тэхнічнае апісаньне”.

Зьвярніце ўвагу: па змаўчаньні, Windows 7 і наступныя вэрсіі загружаюцца з адмысловага невялікага падзелу. Гэты падзел утрымлівае файлы, неабходныя для запуску сыстэмы. Windows дазваляе рабіць запісы ў гэты падзел толькі тым прыкладаньням, якія маюць правы адміністратара (падчас працы сыстэмы). TrueCrypt зашыфруе гэты падзел, толькі калі Вы выберыце для шыфраваньня ўвесь сыстэмны дыск (а ня толькі той падзел, на якім усталяваная апэрацыйная сыстэма).

=====

Сыстэмы, у якіх падтрымліваецца шыфраваньне

У дадзены момант TrueCrypt можа шыфраваць наступныя апэрацыйныя сыстэмы:

- Windows 7 (32-bit і 64-bit)
- Windows Vista (SP1 і пазьнейшыя)
- Windows Vista x64 (64-bit) Edition (SP1 і пазьнейшыя)
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008 R2 (64-bit)
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)

Зьвярніце ўвагу: не падтрымліваюцца наступныя апэрацыйныя сыстэмы (сярод іншых):

- Windows RT
- Windows 2003 IA-64
- Windows 2008 IA-64
- Windows XP IA-64, а таксама Windows Embedded і Tablet Windows.

=====

Схаваная апэрацыйная сыстэма

Можа здарыцца, што Вас прымусяць расшыфраваць апэрацыйную сыстэму. Ёсьць шмат сытуацыяў, калі Вы ня можаце адмовіцца зрабіць гэта (напрыклад, у выпадку вымагальніцтва). TrueCrypt дазваляе стварыць схаваную апэрацыйную сыстэму, існаваньне якой немагчыма даказаць (пры ўмове выкананьня пэўных рэкамэндацыяў).

Такім чынам, Вам ня прыйдзецца расшыфроўваць схаваную сыстэму ці раскрываць пароль да яе. Для атрыманьня дадатковай інфармацыі глядзіце разьдзел “Схаваная апэрацыйная сыстэма” ў главе “Праўдападобнае адмаўленьне”.

Аднаўленчы дыск TrueCrypt

У працэсе падрыхтоўкі шыфраваньня сыстэмнага падзелу ці дыску, TrueCrypt патрабуе стварэньня так званага аднаўленчага дыску (TrueCrypt Rescue Disk) (CD або DVD), неабходнага ў наступных сытуацыях:

Калі вакно TrueCrypt Boot Loader не зьяўляецца пасьля запуску кампутара (або калі Windows не загружаецца), TrueCrypt Boot Loader можа быць пашкоджаны. TrueCrypt Rescue Disk дазваляе аднавіць яго і, такім чынам, вярнуць доступ да шыфраванай сыстэмы і дадзеных (заўважце, аднак, што Вы ўсё роўна павінны ўвесьці правільны пароль). У вакне Rescue Disk абярыце Repair Options> Restore TrueCrypt Boot Loader. Націсьніце ‘Y’ для пацьверджаньня дзеяньня, выньце дыск аднаўленьня з CD/DVD-прываду і перазагрузіце кампутар.

Калі TrueCrypt Boot Loader пашкоджаны або калі Вы ня хочаце, каб ён знаходзіўся на цьвёрдым дыску (напрыклад, калі Вы выкарыстоўваеце альтэрнатыўны загрузьнік/мэнэджар для іншых апэрацыйных сыстэмаў), Вы можаце ажыцьцявіць загрузку наўпрост з аднаўленчага дыску TrueCrypt (бо ён таксама ўтрымлівае загрузьнік TrueCrypt) без аднаўленьня загрузьніка на цьвёрдым дыску. Проста ўстаўце аднаўленчы дыск у CD/DVD-прывад і ўвядзіце пароль у адпаведным акне.

Калі Вы некалькі разоў увялі правільны пароль, але TrueCrypt кажа, што пароль няправільны, верагодна, пашкоджаны майстар-ключ або іншыя крытычныя дадзеныя. TrueCrypt Rescue Disk дазваляе аднавіць

іх і, такім чынам, вярнуць доступ да зашыфраванай сыстэмы і дадзеных (аднак Вам усё роўна прыйдзецца ўвесьці правільны пароль). У вакне аднаўленчага дыску абярыце Repair Options > Restore key data. Увядзіце пароль, націсьніце ‘Y’ для пацьвярджэньня дзеяньня, выміце дыск з CD/DVD-прывада і перазагрузіце кампутар.

Заўважце: гэтая функцыя ня можа быць выкарыстана для аднаўленьня загалоўку схаванага тому, у якім знаходзіцца схаваная апэрацыйная сыстэма. Каб аднавіць такі загаловак тому, націсьніце Select Device, выберыце падзел за абманным сыстэмным падзелам, націсьніце OK, абярыце Tools > Restore Volume Header і кіруйцеся інструкцыямі.

УВАГА: пры аднаўленьні дадзеных ключа з дапамогай TrueCrypt Rescue Disk, Вы таксама аднаўляеце пароль, які быў дзейсным пры стварэньні аднаўленчага дыску. Таму пры зьмене паролю Вы павінны зьнішчыць аднаўленчы дыск TrueCrypt і стварыць новы (абярыце System -> Create Rescue Disk).

У адваротным выпадку, калі зламысьнік ведае Ваш стары пароль (напрыклад, дзякуючы рэгістратару клавіятуры) і знойдзе Ваш стары дыск аднаўленьня TrueCrypt, ён можа выкарыстаць яго для аднаўленьня дадзеных ключа (майстар-ключа, зашыфраванага з дапамогай старога пароля) і, такім чынам, расшыфруе Ваш сыстэмны падзел ці дыск.

Калі Windows пашкоджана і ня можа загрузіцца, аднаўленчы дыск TrueCrypt дазваляе часова расшыфраваць падзел ці дыск перад запускам Windows. У вакне аднаўленчага дыску абярыце Repair Options > Permanently decrypt system partition/drive. Увядзіце пароль і дачакайцеся завяршэньня расшыфроўкі. Па завяршэньні Вы можаце скарыстацца дыскам усталёўкі MS Windows для выпраўленьня загрузкі. Зьвярніце ўвагу, што гэтая функцыя ня можа быць выкарыстана для расшыфроўкі схаванага тому, у якім знаходзіцца схаваная апэрацыйная сыстэма.

ЗАЎВАГА: калі Windows пашкоджана (не запускаецца) і Вам трэба аднавіць яе (або атрымаць доступ да файлаў у ёй), Вы можаце пазьбегнуць расшыфроўкі сыстэмнага падзелу ці дыску наступным чынам.

Загрузіце іншую апэрацыйную сыстэму, запусьціце TrueCrypt, націсьніце Select Device, абярыце няспраўны сыстэмны падзел, выберыце System > Mount Without Pre-Boot Authentication, увядзіце пароль

аўтарызацыі перад загрузкай і націсьніце OK. Падзел будзе змантаваны як звычайны том TrueCrypt (дадзеныя будуць на ляту расшыфраваныя/зашыфраваныя ў апэратыўнай памяці).

Ваш аднаўленчы дыск TrueCrypt утрымлівае рэзэрвовую копію арыгінальнага зьместу першага запісу дыску (зробленага перад тым, як на яго быў запісаны TrueCrypt Boot Loader) і дазваляе пры неабходнасьці яго аднавіць. Першы запіс загрузнага дыску звычайна зьмяшчае сыстэмны загрузьнік або мэнэджар загрузкі. У вакне аднаўленчага дыску абярыце Repair Options > Restore original system loader.

ЗАЎВАЖЦЕ, што нават калі вы згубіце дыск аднаўленьня TrueCrypt і яго знойдзе зламысьнік, ён ня зможа расшыфраваць сыстэмны падзел ці дыск бяз правільнага паролю.

Для загрузкі з дыску аднаўленьня TrueCrypt устаўце яго ў CD/DVD-прывад і перазапусьціце кампутар. Калі на экране ня зьявіцца вакно аднаўленчага дыску (або калі Вы ня бачыце пункту ‘Repair Options’ у разьдзеле ‘Keyboard Controls’ на экране), магчыма, Ваш BIOS настроены на загрузку з жорсткага дыску перад спробай загрузкі з CD/DVD-прывада. Калі гэта так, перазагрузіце кампутар, націсьніце клавішу F2 ці Delete (як толькі ўбачыце стартавы экран BIOS), і пачакайце, пакуль зьявіцца вакно настройкі BIOS. Калі вакно настройкі BIOS не зьяўляецца, перазапусьціце кампутар зноў і націскайце клавішу F2 ці Delete, як толькі перазапусьціце кампутар. Калі зьявіцца вакно настройкі BIOS, абярыце прыярытэт загрузкі з CD/DVD-прывада (для атрыманьня больш падрабязнай інфармацыі, калі ласка, зьвярніцеся да дакумэнтацыі Вашага BIOS/мацярынскай платы або ў службу тэхнічнай падтрымкі пастаўніка Вашага кампутара). Перазагрузіце кампутар. Цяпер мусіць зьявіцца аднаўленчы дыск TrueCrypt. Заўвага: У вакне TrueCrypt Rescue Disk вы можаце абраць ‘Repair Options’, націснуўшы F8 на клавіятуры.

Калі Ваш аднаўленчы дыск TrueCrypt пашкоджаны, Вы можаце стварыць новы, выбраўшы System > Create Rescue Disk. Каб высьветліць, ці пашкоджаны аднаўленчы дыск TrueCrypt, устаўце яго ў CD/DVD-прывад і абярыце System > Verify Rescue Disk.

частка

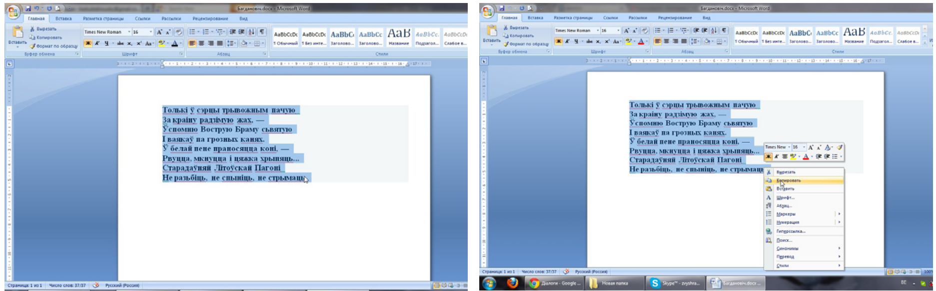
C

GPG/Kleopatra

C

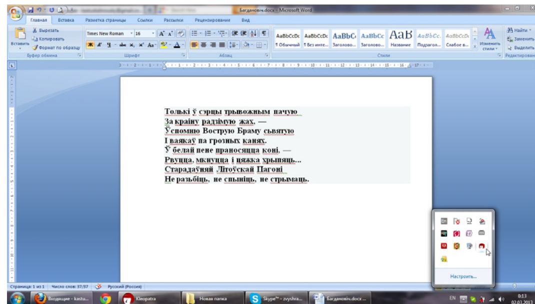
Шыфраваньне тэксту

Трэба выбраць тэкст, які зьбіраемся шыфраваць.

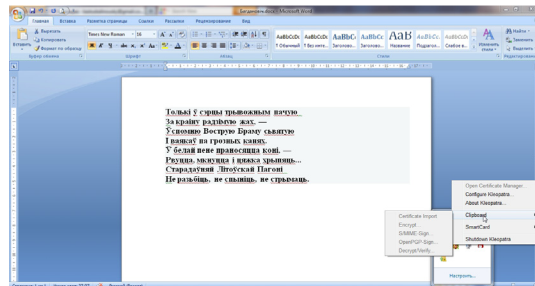


Выдзяліць яго і скапіяваць *(малюнак 1, 2).*

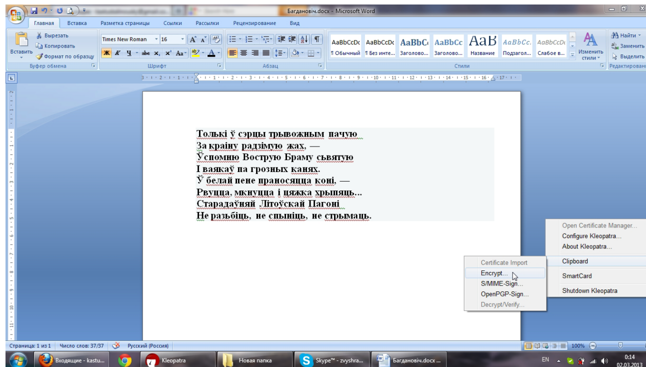
На панэлі задач выбіраем праграму **Kleopatra,** клікаем правай клавішай мышкі *(малюнак 3).*



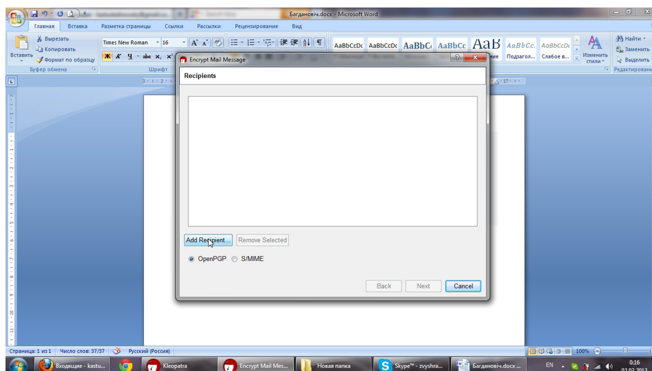
Выбіраем пункт Clipboard *(малюнак 4).*



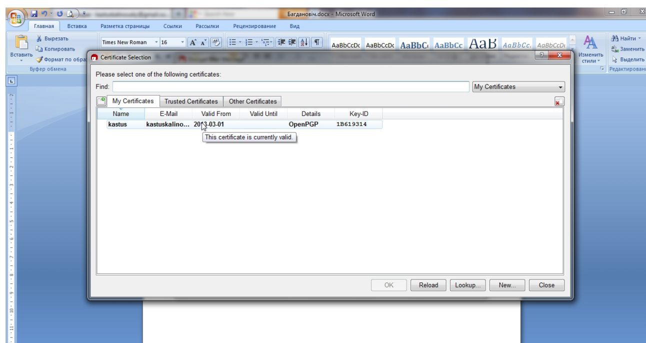
Выбіраем пункт Encrypt *(малюнак 5)*.



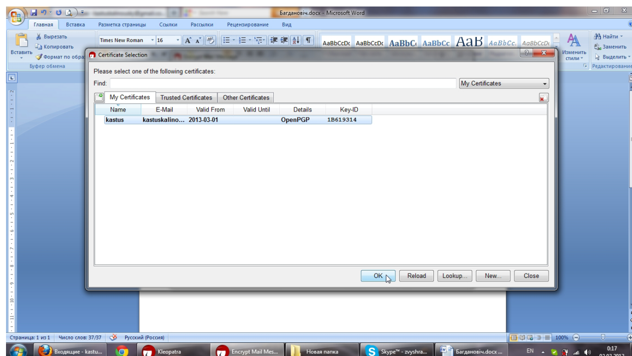
Трэба націснуць Add Recipient, каб дадаць рэспандэнта *(малюнак 6)*.



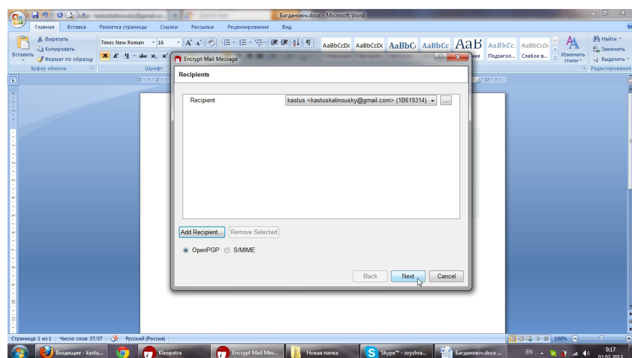
Выбіраем рэспандэнта, для якога трэба зашыфраваць тэкст *(малюнак 7)*.



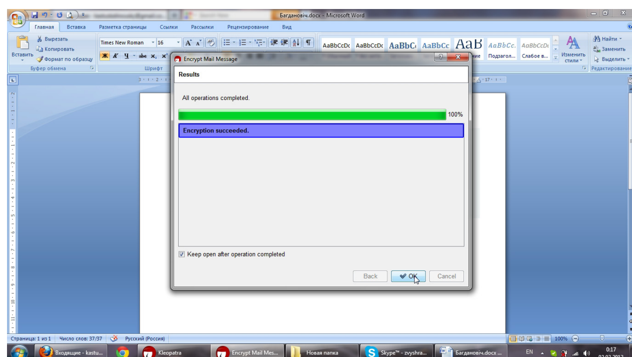
Націскаем OK *(малюнак 8)*.



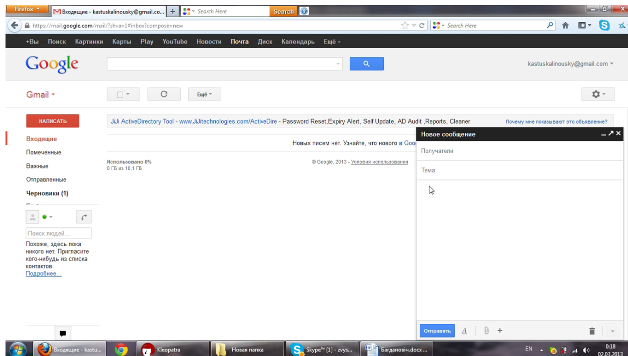
Націскаем Next *(малюнак 9)*.

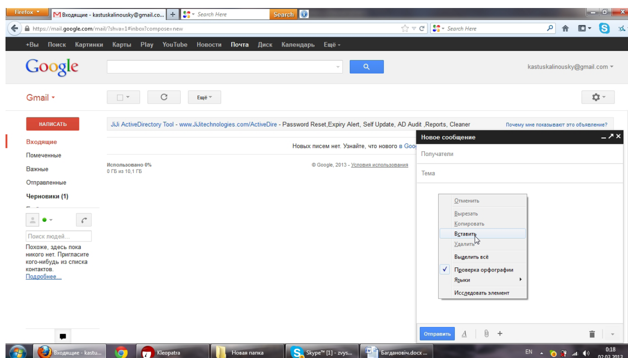


Шыфраванне завершанае. Націскаем OK *(малюнак 10)*.

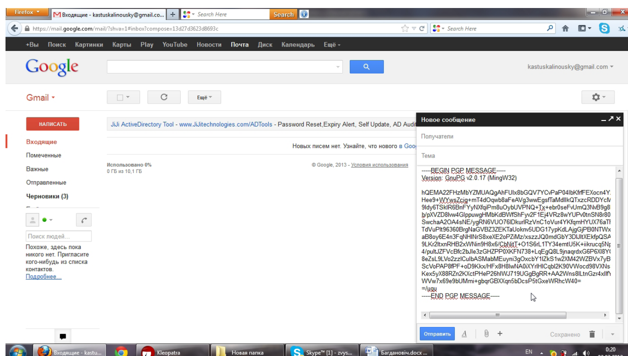


Устаўляем зашыфраваны тэкст у ліст *(малюнак 11, 12)*.

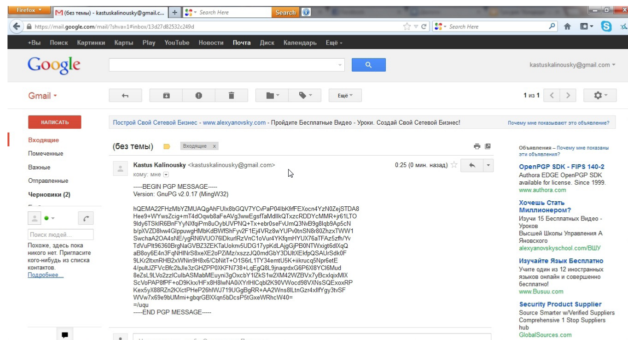




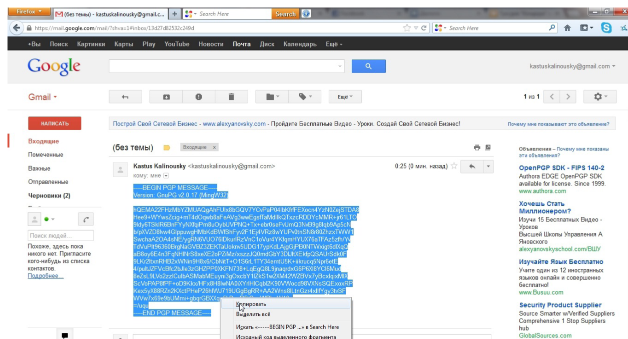
Тэкст зашыфраваны *(малюнак 13)*.



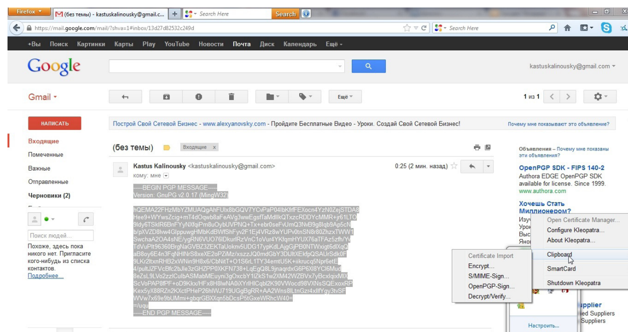
Расшыфроўванне тэксту



Трэба выбраць дасланы зашыфраваны тэкст, які зьбіраемся расшыфраваць, выдзяліць яго і скапіяваць *(малюнак 14, 15)*.

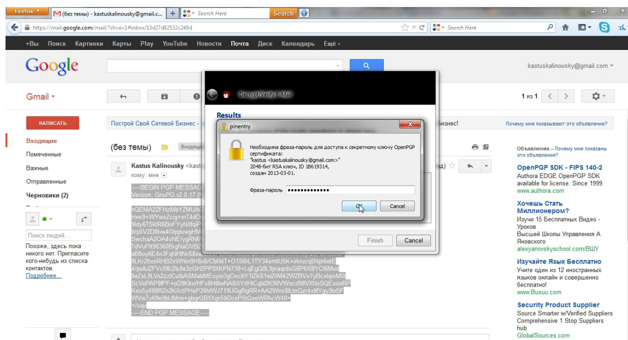


На панэлі задач выбіраем праграму Kleopatra, клікаем правай клавішай мышкі, выбіраем пункт Clipboard *(малюнак 16)*.

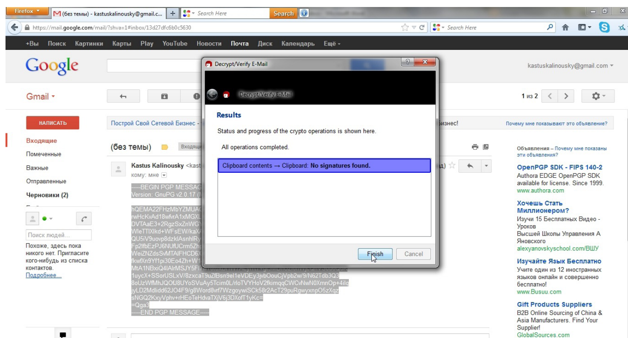


Выбіраем пункт Decrypt/Verify *(малюнак 17)*.

Трэба ўвесьці пароль ад свайго сакрэтнага ключа і націснуць ОК *(малюнак 18)*.

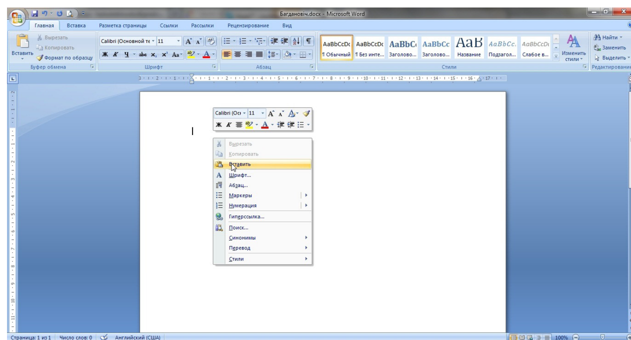


Расшыфроўваньне завершанае.

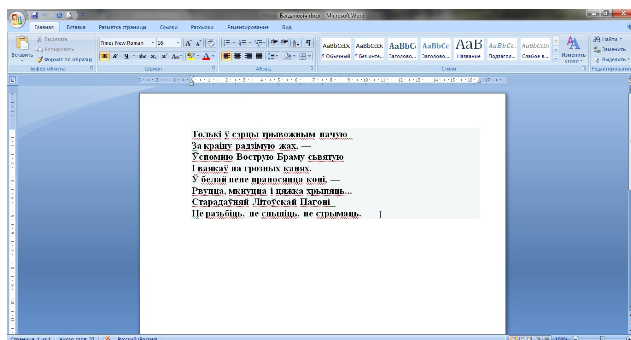


Націскаем Finish *(малюнак 19)*.

Устаўляем расшыфраваны тэкст у тэкставы рэдактар *(малюнак 20)*.

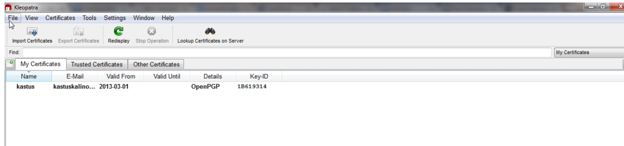


Тэкст расшыфраваны *(малюнак 21)*.

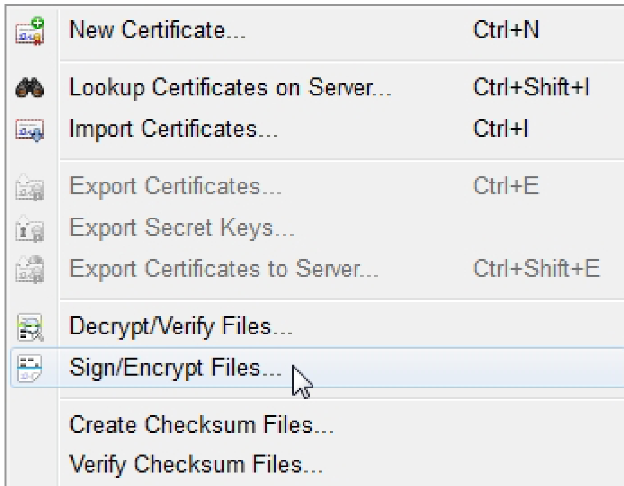


Шыфраваньне файлаў

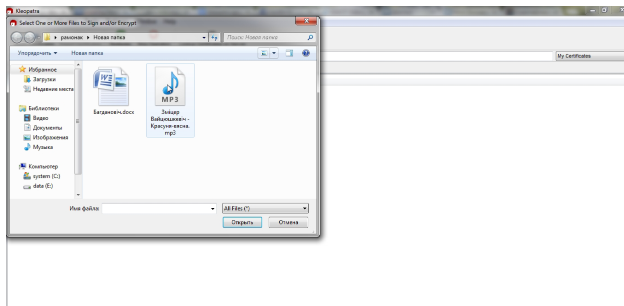
У вакне праграмы Kleopatra трэба выбраць меню File *(малюнак 1)*.



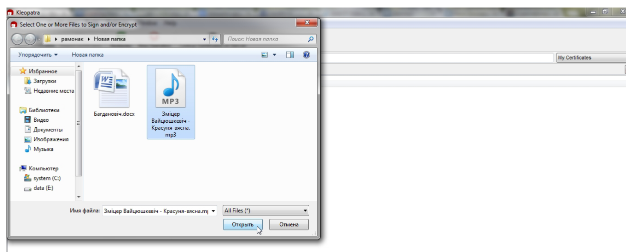
У меню File трэба выбраць пункт Sign/Encrypt Files *(малюнак 2)*.



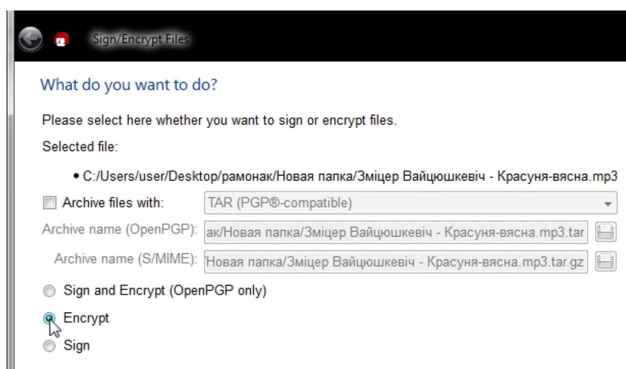
Шукаем файл, які зьбіраемся шыфраваць *(малюнак 3)*.



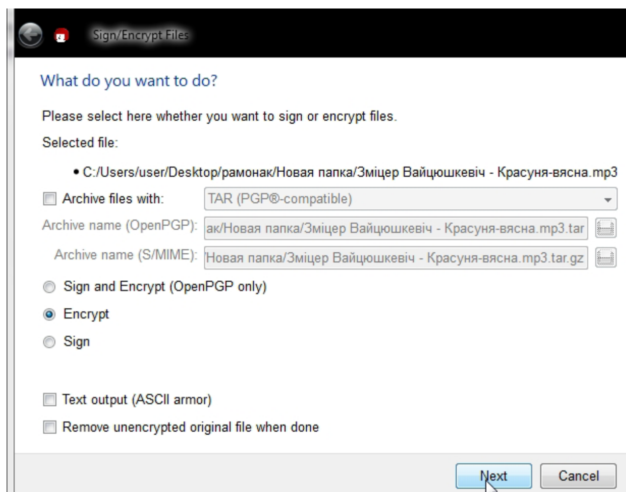
Націскаем “Адчыніць” (малюнак 4).



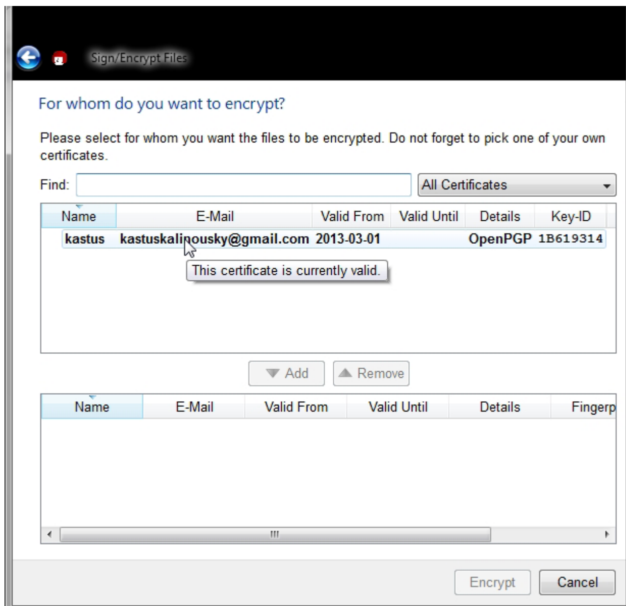
З прапанаваных опцыяў выбіраем пункт Encrypt *(малюнак 5).*

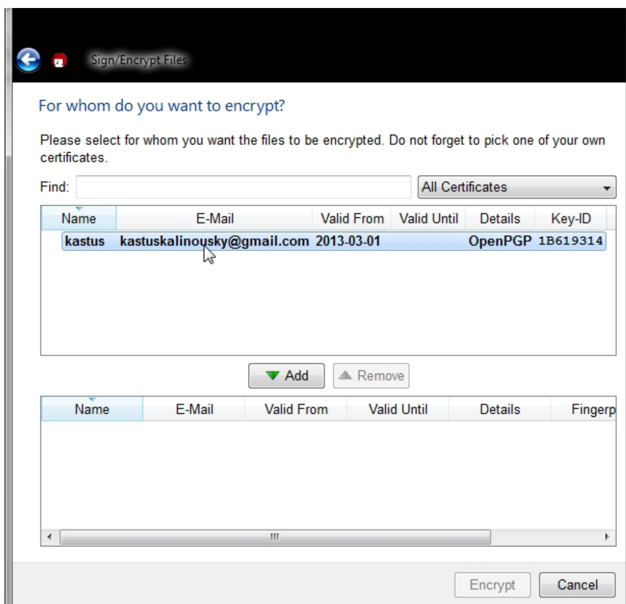


Націскаем Next *(малюнак 6).*

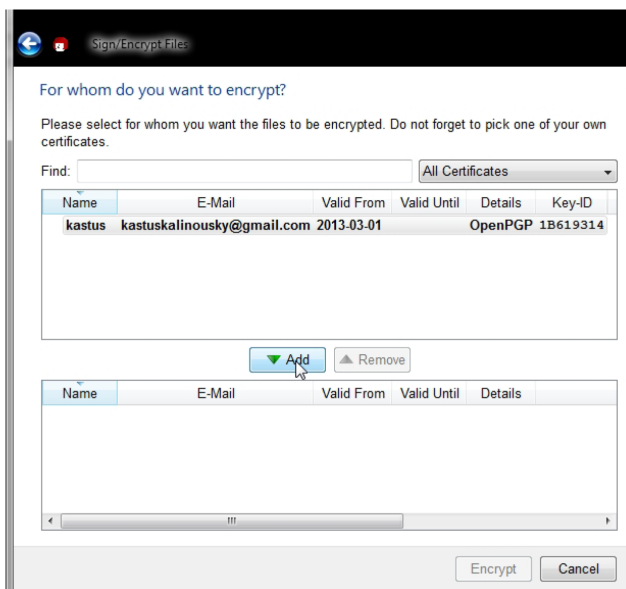


Выбіраем рэспандэнта, для якога трэба зашыфраваць файл (*малюнак 7, 8*).

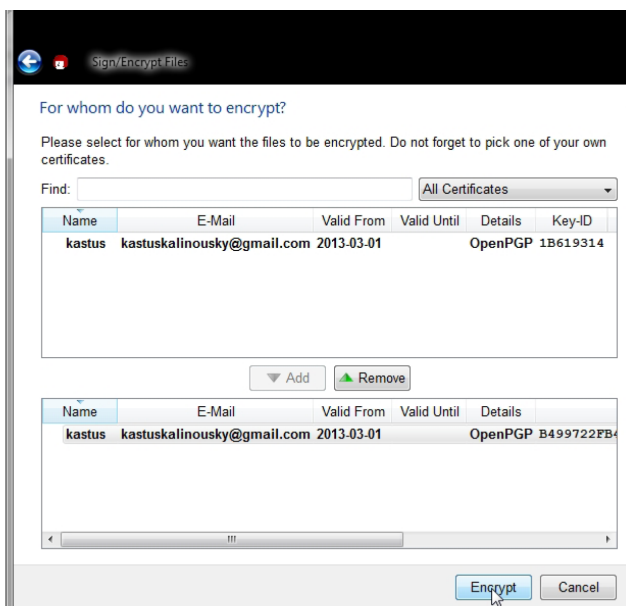




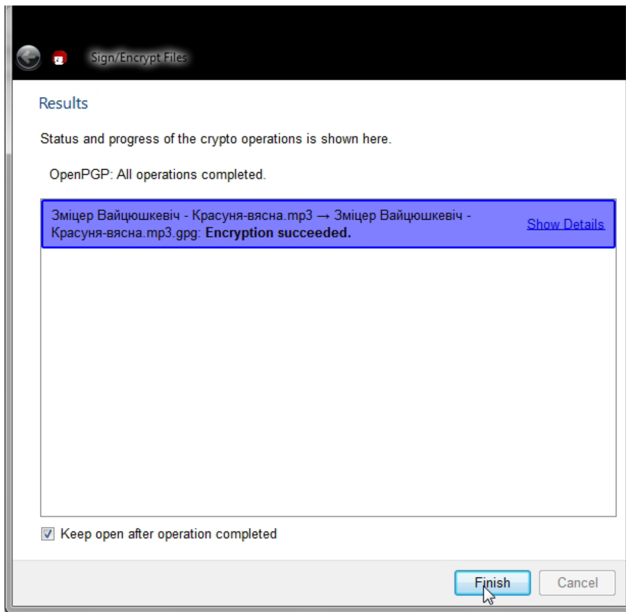
Трэба націснуць Add, каб дадаць рэспандэнта ў сьпіс *(малюнак 9)*.

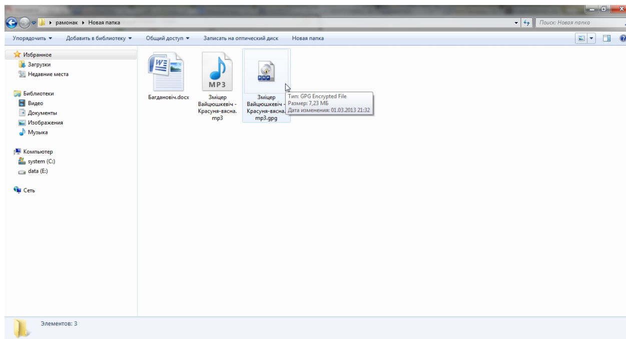


Націскаем Encrypt *(малюнак 10)*.



Шыфраваньне завершанае. Трэба выбраць Finish *(малюнак 11)*.

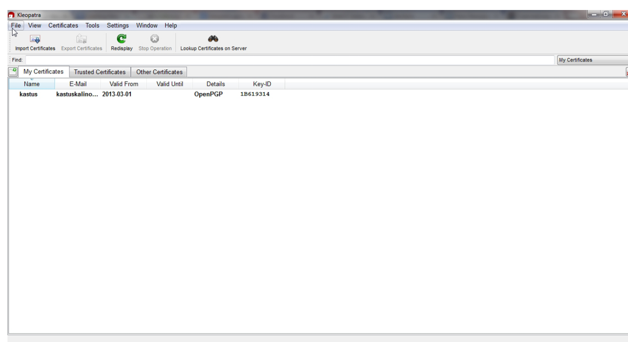




У выніку маем зашыфраваны файл з пашырэньнем gpg *(малюнак 12)*.

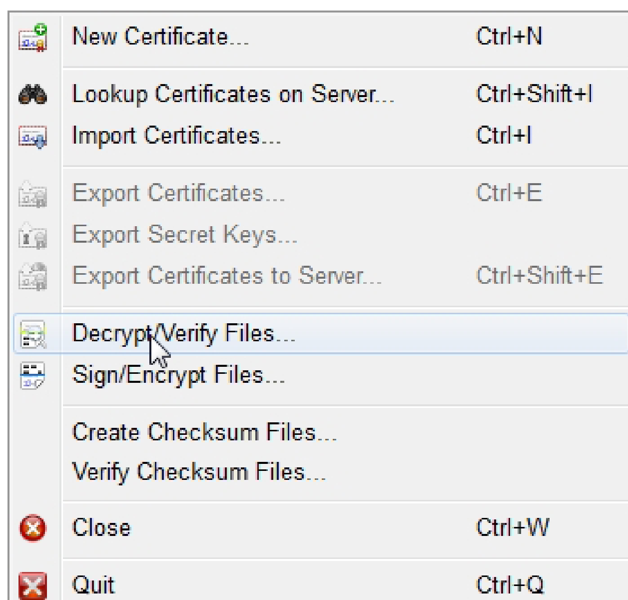
Расшыфроўваньне файлаў

Разгледзім працэс расшыфроўкі файлаў.

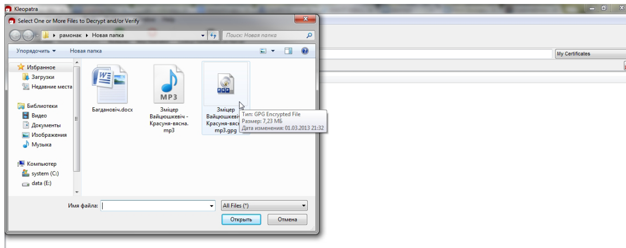


У вакне праграмы **Kleopatra** трэба выбраць меню File *(малюнак 13)*.

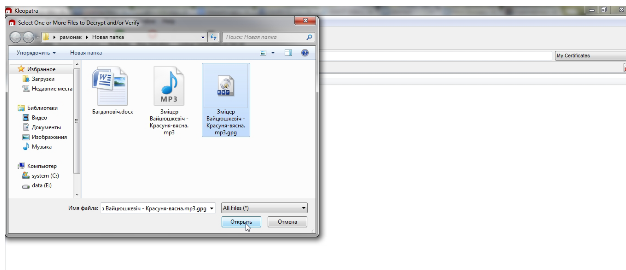
У меню File трэба выбраць пункт **Decrypt/Verify Files** *(малюнак 14)*.



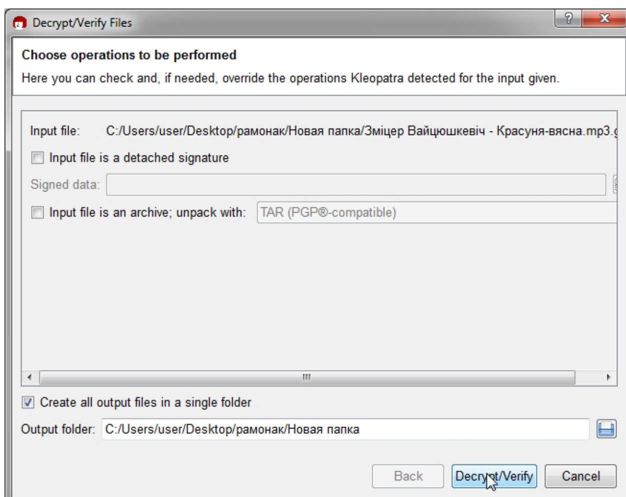
Шукаем і выбіраем зашыфраваны файл, які зьбіраемся расшыфраваць *(малюнак 15)*.



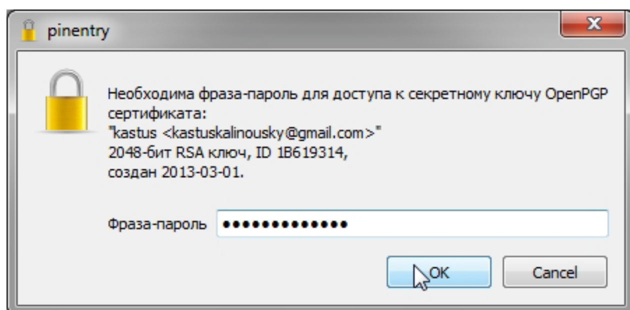
Націскаем “Адчыніць” *(малюнак 16)*.



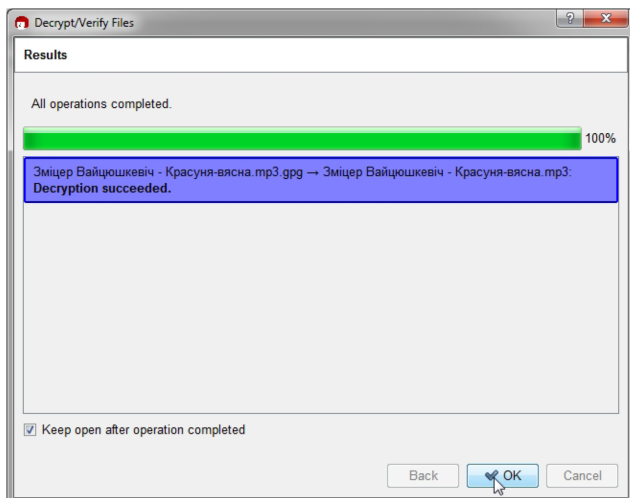
Націскаем **Decrypt/Verify** *(малюнак 17)*.



Уводзім пароль ад свайго сакрэтнага ключа і націскаем ОК *(малюнак 18).*



Расшыфраваньне завершанае *(малюнак 19).*



частка

D

Калі мне трэба выкарыстоўваць Eraser?

Калі мне трэба выкарыстоўваць Eraser?

Вы павінны выкарыстоўваць перазапіс пры дапамозе Eraser кожны раз, калі выдаляеце дадзеныя з дыску. Неабавязкова перазапісваць тыя дадзеныя, якія Вы ня лічыце канфідэнцыйнымі, але няма ніякай шкоды ў перазапісе ўсіх дадзеных, якія Вы выдаляеце.

Аднак існуюць выпадкі, калі перазапіс непрыдатны або можа мець пабочныя эфэкты. Гэтыя выпадкі разглядаюцца ў наступным разьдзеле.

Вы можаце рэгулярна ачышчаць свабоднае месца на дыску, каб пазбавіцца ад рэшткаў часовых файлаў, створаных прыкладаньнямі, і іншай інфармацыі, якая магла быць захаванай на дыску. Можна выкарыстоўваць плянавальнік для запуску гэтай задачы, калі кампутар не выкарыстоўваецца – напрыклад, уначы.

Выключэньні

Сьціснутыя файлы / дыскі

Немагчыма зацерці файлы, сьціснутыя на ўзроўні файлавай сыстэмы (сьціканьне файлаў патрабуе файлавай сыстэмы, якая яго падтрымлівае, напрыклад, NTFS). Файлы, сьціснутыя з дапамогай вонкавага прыкладаньня, такія як ZIP-файлы, можна зацерці, як звычайны файл.

Зашыфраваныя файлы

Немагчыма зацерці файлы, зашыфраваныя на ўзроўні файлавай сыстэмы (шыфраваньне файлаў патрабуе файлавай сыстэмы, якая яго падтрымлівае, напрыклад, NTFS). Аднак файлы, зашыфраваныя з дапамогай вонкавага прыкладаньня, такога як Pretty Good Privacy (PGP) або AxCrypt, можна зацерці.

Паколькі дадзеныя ўжо захоўваюцца ў нечытэльным фармаце, заціраньне непатрэбнае, але звычайна павышае ўзровень бясьпекі (напрыклад, перашкаджае ўзнаўленьню інфармацыі, калі ключ стаў вядомы іншай асобе).

Зашыфраваныя дыскі

Вы можаце зацерці вольную прастору зашыфраваных дыскаў (такіх, як у TrueCrypt) па тых жа прычынах, што і зашыфраваныя файлы. Гэта будзе працаваць, паколькі шыфраваньне зьяўляецца празрыстым для Eraser.

Сеткавыя дыскі

Заціраньне файлаў па сетцы магчымае, але хутчэй за ўсё Eraser ня зможа надзейна зацерці файл, таму што дадзеныя зьмяняюцца праз сеткавы пратакол і сэмантыкі, неабходнай для заціраньня, можа й ня быць. Больш за тое, Вы, хутчэй за ўсё, перагрузіце сетку, што само па сабе неабачліва.

Дыскеты

Дадзеныя на гнуткім дыску можна зацерці так жа, як на жорсткім. Аднак, калі канфідэнцыйная інфармацыя захоўваецца на дыскеце, разгледзьце варыянт яе фізычнага зьнішчэньня.

CD-RW, DVD±RW, цьвёрдацельныя накапляльнікі і г.д.

Такія дыскі маюць абмежаваную колькасьць цыкляў перазапісу, таму, магчыма, Вы захочаце пакінуць заціраньне вольнай дыскавай прасторы для надзвычайных сытуацыяў. Калі носьбіт недарагі (напрыклад, CD-RW), яго можна зьнішчыць фізычна.

D

Ненаўмыснае парушэньне прыватнасьці

Некаторыя дзіры ў бясьпецы, якія найчасьцей выпускаюцца з-пад увагі, прыведзеныя ніжэй.

Файл падпампоўкі

Сховішча віртуальнай памяці апэрацыйнай сыстэмы Windows называецца файл падпампоўкі. Апэрацыйная сыстэма можа захоўваць любую інфармацыю з памяці на дыску, калі ёй гэта патрэбна. Гэта азначае, што файл падпампоўкі можа ўтрымліваць паролі, часткі дакумэнтаў ды іншую канфідэнцыйную інфармацыю.

Падчас сваёй працы апэрацыйная сыстэма блякуе файл падпампоўкі, таму да яго нельга атрымаць доступ пры дапамозе стандартных файлавых апэрацыяў. Існуюць прыкладаньні, якія абяцаюць перазапісаць

файл падпампоўкі, вылучаючы велізарныя аб’ёмы памяці, але ў такім выпадку кампутар можа “завіснуць”, і нават тады нельга атрымаць доступ да прасторы, выдзеленай прыкладаньнямі, як і ня ўся даступная прастора ў файле падпампоўкі абавязкова будзе перазапісаная.

Для атрыманьня інфармацыі аб тым, як ачысьціць файл падпампоўкі, глядзіце разьдзел “Ачыстка файлу падпампоўкі”.

Імёны файлаў

Імя файлу можа раскрыць інфармацыю аб яго зьмесьце, калі, канечне, Вы не даяце файлам адвольныя імёны.

Eraser перазапіша імя файлу пасьля заціраньня дадзеных у ім. Імёны тых файлаў, якія Вы выдалілі раней, могуць па-ранейшаму захоўвацца ў табліцы файлавай сыстэмы. Eraser перазапіша іх, калі Вы будзеце ачышчаць невыкарыстоўваемую дыскавую прастору.

Пашкоджаныя сэктары

Калі вобласьць на дыску па якой-кольвек прычыне пашкоджаная, дыск пазначае, што яна зьмяшчае пашкоджаныя сэктары. Немагчыма атрымаць доступ да такіх сэктараў, таму дадзеныя, якія ўсё яшчэ захоўваюцца ў іх, немагчыма зацерці.

Пітэр Гутман разгледзеў гэтую тэму ў разьдзеле “Праблемы магнітных носьбітаў” сваёй працы “Бясьпечнае выдаленьне дадзеных з магнітных і цьвёрдацельных носьбітаў памяці”.

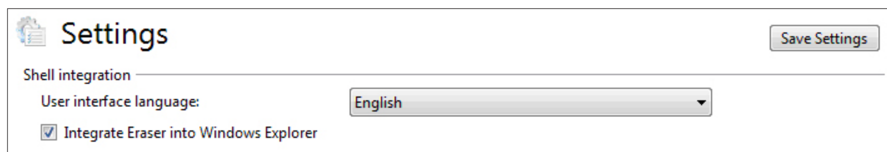
Налады Eraser

Eraser уяўляе сабой наладжвальную праграму, якая дазваляе зьмяняць налады адпаведна Вашым патрабаваньням бясьпекі. Тым ня менш, для большасьці карыстальнікаў той узровень бясьпекі, які прадастаўляюць налады па змаўчаньні, будзе дастатковым.

Заўважце, што для таго, каб налады набылі моц, неабходна націснуць кнопку “Захаваць налады” ў верхняй правай частцы старонкі наладаў. Некаторыя зьмены ў наладах патрабуюць перазагрузкі кампутара.

Інтэграцыя з абалонкай (Shell integration)
Налады Eraser

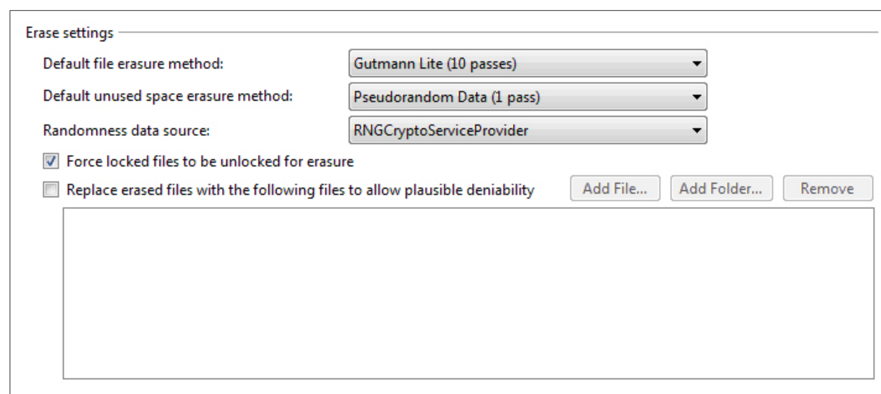
Мова карыстальніцкага інтэрфэйсу вызначае мову інтэрфэйсу Eraser.
Калі стаіць гачок для опцыі “Інтэграваць у праваднік Windows” (Integrate Eraser into Windows Explorer), кантэкстнае мэню праграмы будзе зьяўляцца пры пстрычцы правай кнопкай мышы па элемэнтах у праваднікy.



Налады заціраньня (Erase settings)
налады заціраньня

D

Група “Налады заціраньня” дазваляе задаць паводзіны праграмы пры



заціраньні файлаў.
Калі ў мэтах задачы ўказаны мэтад заціраньня “па змаўчаньні”, будзе ўжыты Мэтад па змаўчаньні для заціраньня файлаў (Default file erasure method) і Мэтад па змаўчаньні для заціраньня вольнай прасторы (Default unused space erasure method).
Крыніца выпадковасьці дадзеных (Randomness data source) паказвае

адкуль атрымліваць выпадковыя дадзеныя для выкарыстаньня падчас заціраньня.

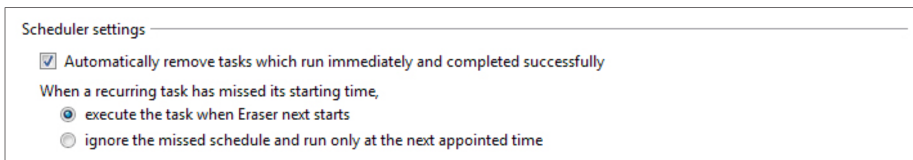
Калі стаіць гачок для опцыі “Прымусова разблякаваць заблякаваныя файлы дзеля заціраньня” (Force locked files to be unlocked for erasure), калі Eraser спрабуе зацерці файл, але ён заблякаваны пэўным прыкладаньнем, праграма прымусова разблякуе гэты файл для заціраньня. Калі гачок зьняты, Eraser праігнаруе файл і паведаміць аб памылцы.

Опцыя “Замяніць сьцёртыя файлы наступнымі файламі дзеля праўдападобнага адмаўленьня” (Replace erased files with the following files to allow plausible deniability) вызначае сьпіс файлаў , якія будуць выкарыстаныя для запаўненьня прасторы сьцёртых файлаў на дыску, каб стварыць уражаньне, што ніякія файлы не былі зьнішчаныя, за выключэньнем іншых файлаў, якія былі выдаленыя папярэдне (адсюль праўдападобнае адмаўленьне).

Налады плянавальніка (Scheduler settings)

налады плянавальніка

Калі выбраная опцыя “Аўтаматычна выдаляць задачы, якія выконваюцца неадкладна і пасьпяхова завершаныя” (Automatically remove tasks which run immediately and completed successfully), задачы, заплянаваныя на неадкладны запуск і завершаныя без памылак, аўтаматычна вы-



даляюцца з плянавальніку заціраньня.

Наступныя два пераключальнікі вызначаюць паводзіны пэрыядычных задачаў, калі час іх запуску быў прапушчаны:

“Выканаць задачу пры наступным запуску Eraser” (execute the task when Eraser next starts) выкліча выкананьне задачы, калі Eraser будзе запушчаны ў наступны раз.

“Праігнараваць прапушчаны тэрмін і выканаць задачу толькі ў наступны прызначаны час” (ignore the missed schedule and run only at the next appointed time) прывядзе да пераносу выкананьня задачы, як калі б яна была выкананая па раскладзе.

Плагіны (Plugins)
плагіны

Разьдзел “Плагіны” зьмяшчае сьпіс плагінаў, якія загружаныя ў Eraser.

Асноўныя плагіны (Core plugins) – гэта плагіны, якія ня могуць быць адключаныя.

Выява ключа побач зь імем плагіну азначае, што плагін падпісаны.

Падпісаным плагінам аўтаматычна дазволена запускацца пасьля ўсталёўкі.

Непадпісаныя плагіны павінны быць абавязкова праверааныя карыстальнікам.

Plugins

Name	Author	Version	File Path
Core plugins			
Default Erasure Methods and PRNGs	The Eraser Project <er...	6.0.5.1158	D:\Development\Projects\Era...

Гачок побач зь імем паказвае, ці будзе плагін загружацца ў будучыні (калі гачок зьняты, плагін адключаны).

Пстрычка правай кнопкай мышы па плагіне адлюструе кантэкстнае мэню з Наладамі, калі плагін мае дадатковыя налады.

Выкарыстаньне пашырэньня правадніку Windows

Калі падчас усталёўкі Вы абралі пашырэньне правадніку Windows, Eraser дадасьць пункт кантэкстнага мэню пры пстрычцы правай кнопкай мышы па наступных элемэнтах:

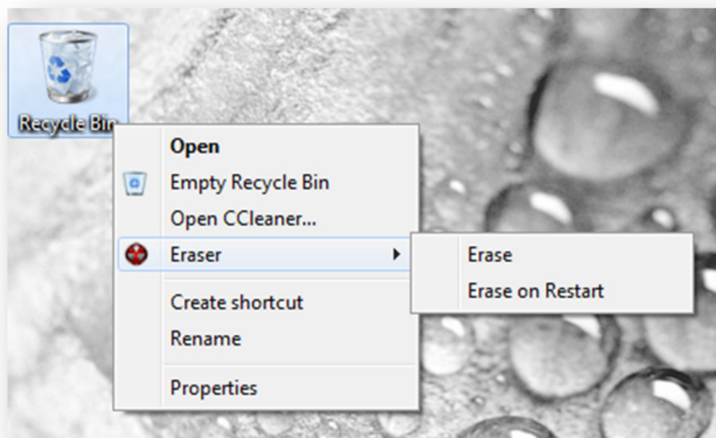
- Файлы і/ці тэчкі
- Дыскі ў тэчцы “Кампутар”
- Кошык

Пры навядзеньні курсору на мэню Eraser адкрыецца падмэню, якое зьмяшчае элементы “Зацерці” (Erase) і “Зацерці пры перазагрузцы” (Erase on Restart). Калі пстрыкнуць правай кнопкай мышы па дыску, у Вас зьявіцца магчымасьць “Зацерці свабодную прастору” (Erase unused space) з кантэкстнага мэню. Калі ў кошыку няма файлаў, кантэкстнае мэню Eraser будзе адлюстроўвацца шэрым колерам.

Выбар любой з опцыяў адправіць новую задачу запушчанай праграме Eraser (або яна будзе запушчана), а ў вобласьці апавяшчэньняў сыстэмы зьявіцца апавяшчэньне, калі задача будзе выкананая.

Ачысьціць кошык

Опцыя 1: Выкарыстоўваючы пашырэньне праваднiку Windows



- Перайсьці на працоўны стол
- Пстрыкнуць правай кнопкай мышы па кошыку
- Выбраць Eraser | Зацерці (Erase)

частка

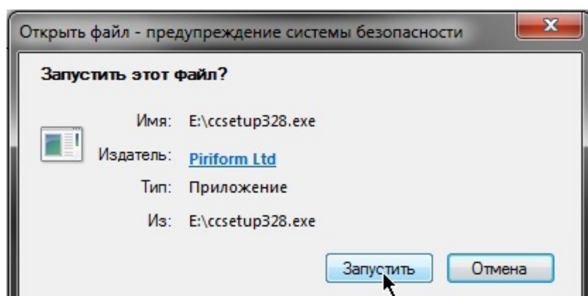
E

CCleaner

E

CCleaner

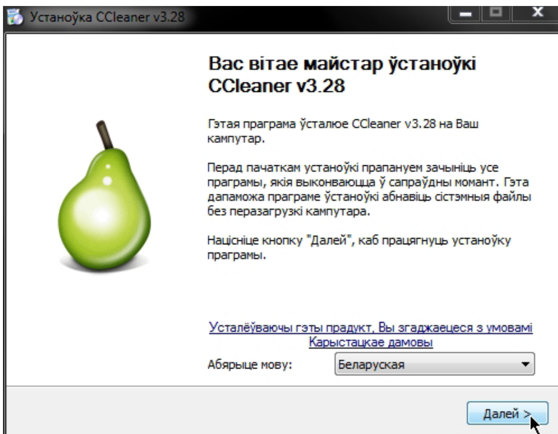
Запускаем файл ccsetup328.exe, каб усталяваць праграму CCleaner. Націскаем “Запустить” *(малюнак 1)*.



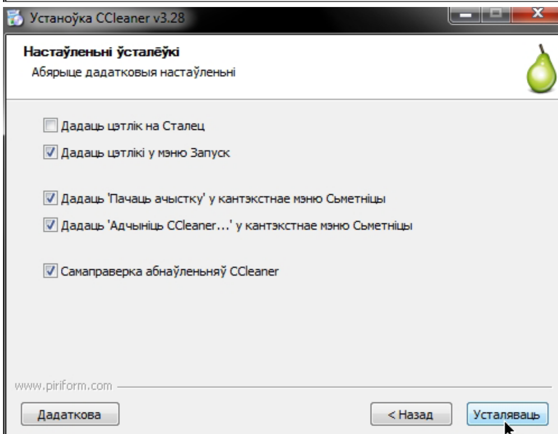
Выбіраем мову праграмы, напрыклад, беларускую *(малюнак 2, 3)*.



Далей трэба націснуць «Next» *(малюнак 4).*



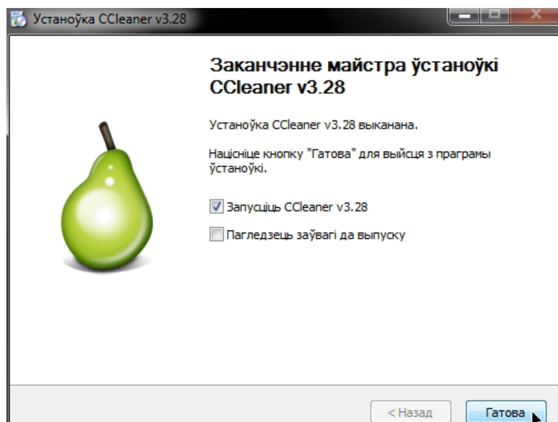
Памянялася мова праграмы. Націскаем "Далей" *(малюнак 5).*



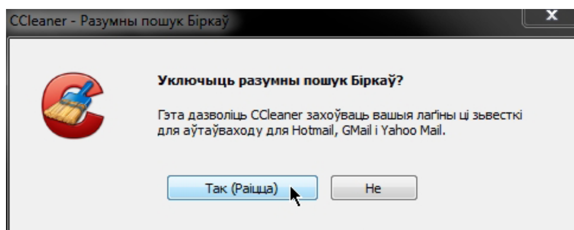
Выбіраем неабходныя наладкі і націскаем "Усталяваць" (малюнак 6).

E

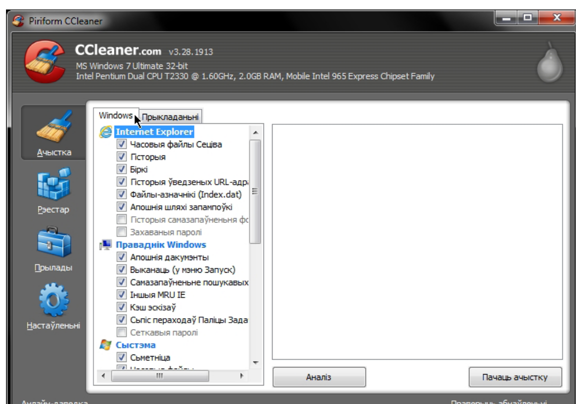
Праграма ўсталявана. Націскаем “Гатова” *(малюнак 7)*.

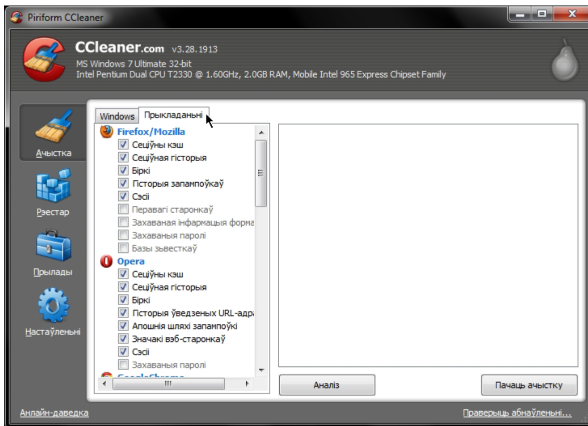


У наступным кроку выбіраем пункт у залежнасьці ад уласных патрэбаў, напрыклад, “Так” *(малюнак 8)*.

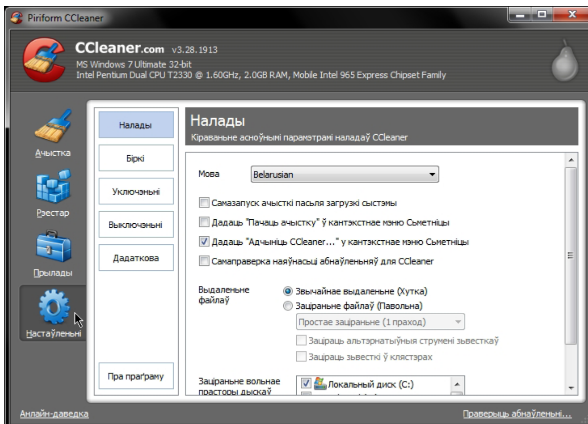


У вакне праграмы ў закладцы Windows выбіраем неабходныя для ачысткі пункты *(малюнак 9)*.

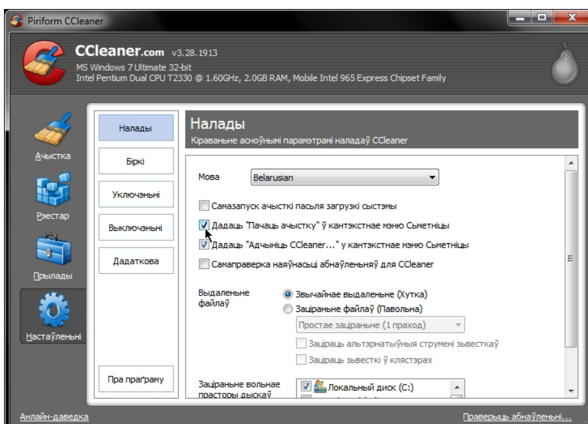




У вакне праграмы ў закладцы Прыкладаньні выбіраем неабходныя для ачысткі пункты *(малюнак 10).*

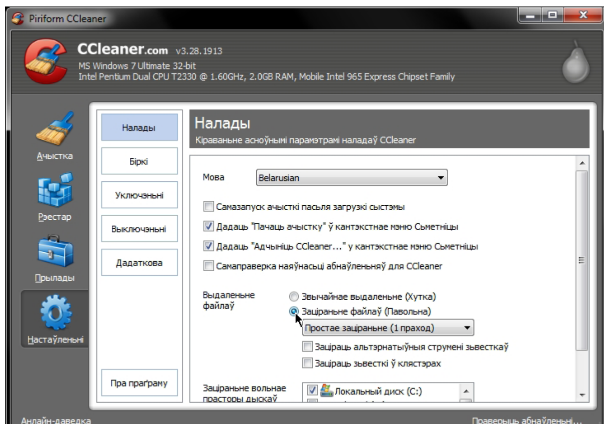


Выбіраем апошні пункт мэню “Настаўленьні” для таго, каб наладзіць якасць выдаленьня *(малюнак 11).*

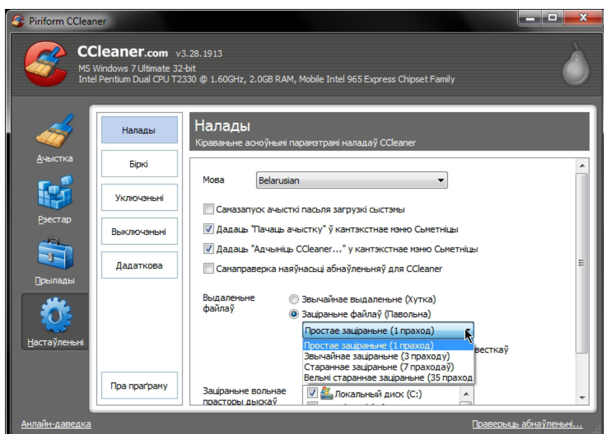


Дадаем “Пачаць ачыстку” *(малюнак 12).*

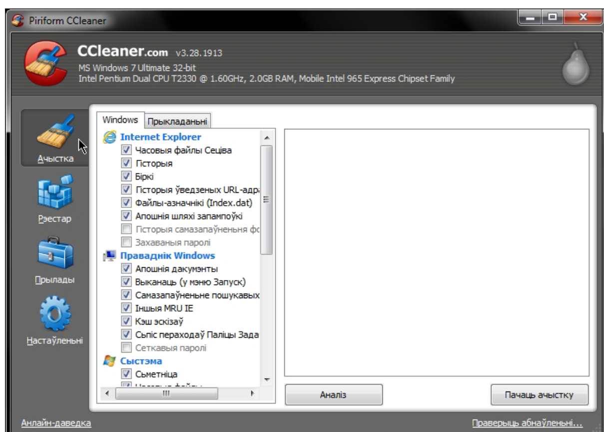
E



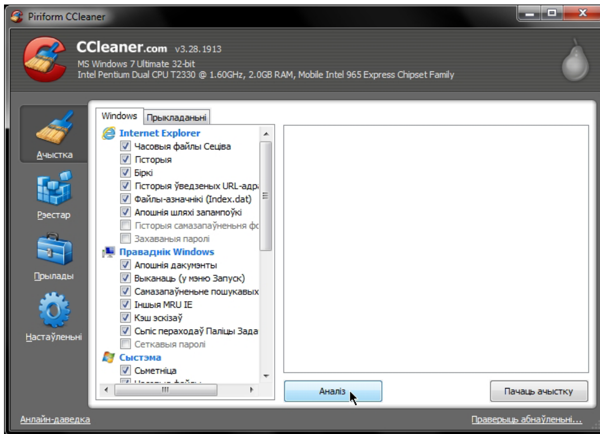
У пункце «Выдаленьне файлаў» выбіраем Заціранне файлаў *(малюнак 13).*



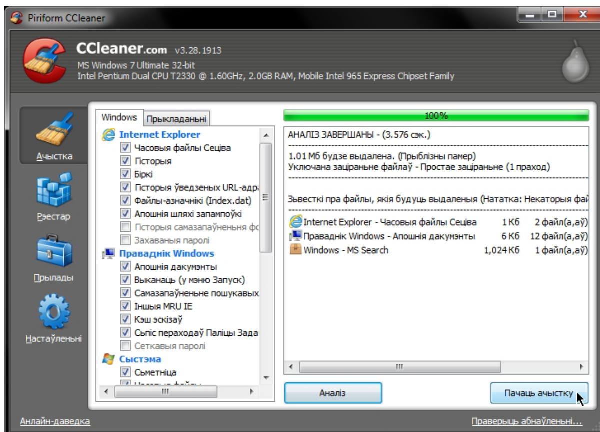
З прапанаваных варыянтаў выбіраем неабходны, напрыклад, “Простае заціраньне (адзін праход)” *(малюнак 14).*



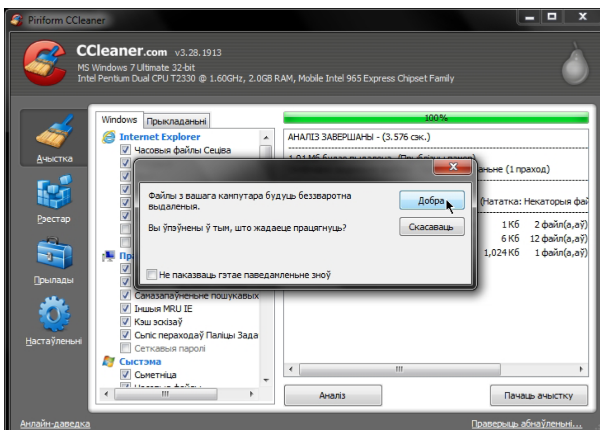
Выбіраем пункт мэню Ачыстка *(малюнак 15).*



Націскаем на “Аналіз” *(малюнак 16).*

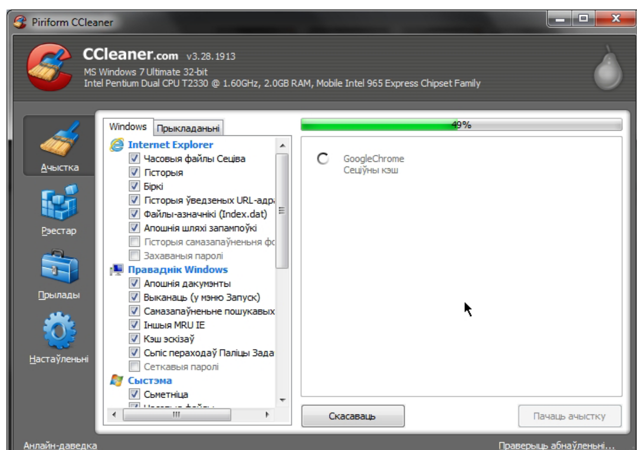


Аналіз завершаны. Націскаем Пачаць ачыстку *(малюнак 17).*

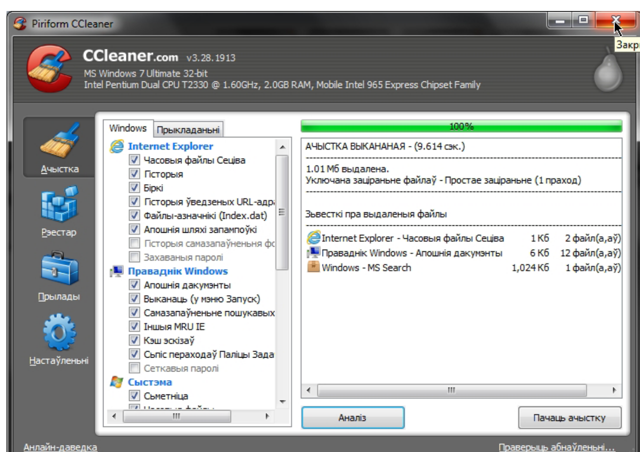


Націскаем “Добра” *(малюнак 18).*

E



Адбываецца ачыстка *(малюнак 19).*



Ачыстка выкананая *(малюнак 20).*

частка

F

Агляд іншых карысных праграмаў ды сайтаў

Агляд іншых карысных праграмаў ды сайтаў

KeePass

У сучасным сьвеце вам трэба запамінаць мноства пароляў. Вам патрэбныя паролі для ўваходу ў сыстэму Windows, да вашай электроннай паштовай скрыні, да FTP вашага вэб-сайту, анляйн паролі (накшталт паролей да ўліковых запісаў на вэб-сайтах) і гэтак далей. Гэты сьпіс бясконцы. Пры гэтым вы павінныя выкарыстоўваць розныя паролі да кожнага ўліковага запісу. Бо, калі вы выкарыстоўваеце адзін пароль паўсюль, і нехта атрымае гэты пароль, у вас будуць праблемы, сур’ёзныя праблемы. Злодзей будзе мець доступ да вашай электроннай паштовай скрыні, да вашага вэб-сайту і гэтак далей. Проста катастрофа.

Keepass – гэта бясплатны мэнэджар пароляў, які ёсьць у адкрытым доступе, і які дапамагае вам бясьпечна кіраваць вашымі паролямі.

Вы можаце захаваць усе вашыя паролі ў адной базе дадзеных, якая зачыняецца пры дапамозе аднаго ключа майстра альбо ключавога файлу. Так, вам патрэбна будзе запомніць толькі адзін пароль майстра альбо выбраць ключавы файл, каб адчыніць усю базу дадзеных. База дадзеных шыфруецца з дапамогай найлепшых і самых бясьпечных альгарытмаў шыфраваньня, якія існуюць на сёньняшні дзень (такія як AES і Twofish).

keepass.info

Tor



Tor – гэта сетка віртуальных тунэляў, якая дазваляе людзям і групам павысіць прыватнасьць і бясьпеку ў Інтэрнэце. Ён таксама дазваляе распрацоўшчыкам праграмнага забесьпячэньня ствараць новыя камунікацыйныя прылады з убудаванымі параметрамі прыватнасьці.

Tor зьяўляецца асновай для шэрагу прыкладных праграмаў, якія дазваляюць арганізацыям і прыватным асобам дзяліцца

інфармацыяй праз сеткі агульнага карыстаньня, не ахвяруючы пры гэтым прыватнасьцю.

Прыватныя асобы карыстаюцца Tor, каб нельга было адсачыць, якія сайты наведваюць яны альбо іх родныя, а таксама, каб наведваць навінныя сайты, сэрвісы імгненнага абмену паведамленьнямі і ўсё тое іншае, што блякуецца іх мясцовымі Інтэрнэт правайдэрамі.



Схаваныя сэрвісы Tor дазваляюць карыстальнікам публікаваць вэбсайты ды іншыя сэрвісы без магчымасьці адсачыць месцазнаходжаньне сайту.

Прыватныя асобы таксама выкарыстоўваюць Tor для сацыяльна адчувальнай камунікацыі, напрыклад, для чатаў і Інтэрнэт форумаў для ахвяраў гвалту і абразаў альбо для людзей, пакутуючых на хваробы.

Журналісты выкарыстоўваюць Tor для больш бяспечнай камунікацыі з грамадзкімі актывістамі і дысыдэнтамі. Няўрадавыя арганізацыі (НДА) выкарыстоўваюць Tor дзеля таго, каб іх супрацоўнікі маглі заходзіць на свае хатнія вэб-сайты ў той час, калі яны знаходзяцца за мяжой, і ўсе тыя, хто знаходзіцца побач, не маглі заўважыць, што яны супрацоўнічаюць з гэтай арганізацыяй.

Групы актывістаў могуць карыстацца Tor дзеля таго, каб забясьпечыць анляйн прыватнасьць і бясьпеку сваіх сябраў.

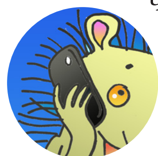
Карпарацыі выкарыстоўваюць Tor як бясьпечны сродак правядзеньня канкурэнтных аналізаў і як сродак абароны важнай інфармацыі ад прыладаў перахопу паведамленьняў. Яны таксама яго выкарыстоўваюць як замену віртуальным прыватным сеткам, якія раскрываюць інфармацыю аб дакладнай колькасьці і часе камунікацыі. У якіх месцах супрацоўнікі працавалі больш за працоўны дзень? У якіх месцах супрацоўнікі наведваюць сайты па пошуку працы? Якія навуковадасьледчыя дэпартамэнты камунікуюць зь юрыстамі-патэнтазнаўцамі кампаніі?

Філія ВМС ЗША выкарыстоўвае Tor дзеля збору выведдадзеных, а адно зь іх падраздзяленьняў карысталася ім падчас нядаўняга разгортваньня на Бліжнім Усходзе. Праваахоўныя органы выкарыстоўваюць Tor дзеля наведваньня альбо назіраньня за сайтамі, каб не пакідаць

F

дзяржаўныя IP-адрэсы ў сеткавым логу, і дзеля бясьпекі падчас апэрацыяў пад прыкрыцьцём.

Шырокае кола людзей, якія карыстаюцца Tor, насамрэч зьяўляецца часткай таго, што робіць яго такім бясьпечным. Tor хавае вас сярод іншых карыстальнікаў сеткі, таму чым больш шырокай і разнастайнай будзе база карыстальнікаў Tor, тым лепш вашая ананімнасьць будзе абароненая.



Мы рэкамэндуем часьцей спраўджваць абнаўленьні на сайце праекту.

torproject.org

Unison

Unison — гэта сынхранізатар файлаў. Гэта дапамагае лягчэй рабіць рэзэрвовыя копіі (бэкапы), ці проста працаваць зь некалькімі вэрсіямі аднаго каталёгу (напрыклад, на стацыянарным кампутары і лэптопе, на кампутары і флэшцы).

Вы ўносілі зьмены і там, і тут — і цяпер вам складана разабрацца, дзе апошняя вэрсія, ці трэба скапіяваць файлы з A на B, ці наадварот? Unison можа дапамагчы.



Праграма паспрабуе вызначыць дзе сьвежыя абнаўленьні, а дзе састарэлая копія. У выпадку канфліктных зьменаў — гэта, калі, напрыклад, адзін і той жа файл у каталёгу быў асобна адрэдагаваны і на флэшцы і на кампутары — Unison папярэдзіць вас, і вы ня згубіце праўкі.

Праграма працуе на Windows і Unix-like сыстэмах.

http://www.cis.upenn.edu/~bcpierce/unison

Witness

Гэта міжнарожны праект, створаны, каб навучыць людзей выкарыстоўваць мультымэдыйныя магчымасьці вашага тэлефону — камэру і мікрафон, каб рабіць грамадзянскія рэпартажы, фіксаваць факты парушэньня закону, ці правоў. Сайт праекту прапаноўвае навучальныя матэрыялы і гісторыі дасьведчаных карыстальнікаў.

Witness.org

Дапаможнік Вожыка-актывіста

Усталяваньне і выкарыстаньне праграмаў, карысных для бясьпекі





Гэтае выданьне зьяўляецца працягам і разьвіцьцём “Кансьпіратара Беларускага” – дапаможніка для грамадзкіх актывістаў, упершыню выдадзенага ў 2005 г.

Мы дзякуем за дапамогу ў ажыцьцяўленьні праекту калегам са славацкай грамадзкай арганізацыі Človek v ohrození.

Наклад 299 асобнікаў.

Дапаможнік Вожыка-актывіста

Усталяваньне і выкарыстаньне праграмаў, карысных для бясьпекі





